

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 01 6:26 PM  
**To:** la-al@justice.gc.ca  
**Subject:** reply

s.19(1)

this is ridiculous and shouldn't happen !!!!!!!!!!!!!

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 01 1:56 AM  
**To:** la-al@justice.gc.ca  
**Subject:** gov. internet Stalinists

s.19(1)

Re:gov plans to spy on Canadian internet users

Don't you guys have enough real problems to deal with in the country without meddling in the private homes of Canadians?

I can think of some examples like Health Care, Canada U.S. softwood lumber negotiations, Free trade, modernizing legislation affecting First Nations life in Canada etc., etc.

We need more freedom in this country and less Stalinism. Am I to expect visitors in the middle of the night to take me away as a result of this E-mail?

Concerned



**Pierlot, Paul**

s.19(1)

**From:** [REDACTED]  
**Sent:** 2002 Sep 02 12:07 AM  
**To:** la-al@justice.gc.ca  
**Cc:** Letters@GlobeAndMail.ca; metatron@escape.ca  
**Subject:** Proposals in "Lawful Access -- Consultation Document"

The Canadian Department of Justice document entitled "Lawful Access - Consultation Document" [online at [http://www.canada.justice.gc.ca/en/cons/la\\_al/](http://www.canada.justice.gc.ca/en/cons/la_al/)] is so outrageous from beginning to end that it is hard to know where to begin to criticize it. One is left spluttering and stammering at the sheer effrontery.

It suggests that ISPs might be required to become proxy law enforcement agents, a role for which they are emphatically not suited. Nor has the slightest thought apparently been given to public accountability for this process, which would be so easily open to abuse.

It proposes making the mere possession of a computer virus a criminal offense, whether or not it has been deployed or has caused any mischief! This not only fails to account for the fact that viruses can be and indeed, by their very nature, nearly always are present on a computer against the will of that computer's owner, it would also render research on combating new viruses illegal -- which is surely against the public interest.

It proposes a national database cross-referencing email addresses with name and address information. On the internet, people can discuss sensitive personal issues such as sexual orientation or recovery from trauma in support groups, from the safety of an anonymous email identity. Often free web-mail addresses are used, where the individual can easily supply a fictitious name and address.

Naturally, criminals can use web-mail addresses too; the proposed database would be useless if it could be so easily circumvented. But if the database is to contain a complete list of all email addresses ever used by an individual, that could only be obtainable by intercepting all the Web surfing that every Canadian does! Unless, of course, having an anonymous email address is going to be outlawed...

However acquired, this would be a dangerous accumulation. Can the bureaucrats making this proposal guarantee for all time that this highly sensitive database could never, ever be hacked, its contents released to the Internet at large? Of course not. Computer security is an arms race; precautions that are good enough today become inadequate tomorrow. The damage, once done, could never be undone. Against the danger of creating such a sword to dangle over the privacy of all Canadians, some of whom would be irretrievably injured by that release, what counter benefit is cited? An improbable case where authorities have only an email address, and wish to contact the next-of-kin. How often is an email address going to be the sole identifying piece of information available about an injured person? Should that be a justification for allowing the invasive process of accumulating that database?

The paper also proposes gutting the safeguards currently provided in the Criminal Code against general fishing expeditions into the affairs of private citizens in cases where there are no reasonable grounds to believe that an offense either has been or will be committed.

There is a slippery slope: once legal authority is granted for government to monitor an aspect of citizens' communications under some circumscribed circumstances, it then becomes easier for them to argue that there is no reasonable expectation of privacy in that mode of communication, and to extend the monitoring to more and more invasive situations. The danger of this is particularly acute now, because of September 11th.

Terrorism is not a short-term threat that can be "defeated" once and for all, after which we will all somehow go back to living as we did before. War is a false metaphor, because wars \_end\_. Whatever changes we institute to fight terrorists, we will have to live with our whole lives long. We must make sure that, in our haste to deal with what seems like an emergency, we do not consent to give up the qualities that make us Canadian.

Could a bill based on this paper help catch terrorists? Maybe, a little bit. If we all had to live our lives under 24-hour surveillance cameras monitored by thought police, that would probably help too. Once a right has been surrendered, it is exceedingly hard to get it back. Where are we going to draw the line?

There will always be forces pressuring governments to infringe on the rights of their citizens; there will always be excuses for stealing yet another expectation of privacy.

Let us hope there will always be Canadians willing to speak out against such trespasses.

I can sum up my response to this badly-conceived proposal in one sentence: Let it die.



s.19(1)

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Sep 02 3:45 PM  
To: la-al@justice.gc.ca  
Subject: Lawful Access - Consultation Document

Please note my comments on various sections of the document.

Re the section titled "Orders to obtain subscriber and/or service provider information", the statement is made:

"The *Personal Information Protection and Electronic Documents Act* allows for the disclosure of personal information without the knowledge and consent of the individual to whom it pertains, as long as that disclosure is requested by a government institution that has identified its lawful authority to obtain such information."

I believe there is a growing sense in the public domain, in the face of an unprecedented assault on privacy in this electronic age, that personal information disclosure should be much more severely limited. It was once said that "If two people know something, it is no longer a secret." This is clearly hyperbole, but comes from the common sense notion that privacy is at risk when too many people/agencies with non-imperative reasons for inspection have access to personal information. While it may be excessive to require search warrants for address and identification information, the range of purposes and agencies associated should be clearly spelled out and limited.

Further, in response to the statement that

"A problem does exist in cases where no warrant can be obtained under the *Criminal Code* (e.g., s. 487) because law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation.",

I posit that if there is insufficient reason to gain such a warrant, then no such access should be provided. "Early stages of an investigation" could be interpreted as "fishing expedition", which is clearly disallowed under the standards to obtain a warrant. If there are insufficient grounds to obtain a warrant, there are insufficient grounds to require breach of privacy. The representation re location of next of kin is clearly specious, as it is difficult to conceive a situation where internet access can be related to such an emergency.

It would seem reasonable to relate an assistance order to proper search warrants, although the cost to the service provider should be considered. A reasonable analogy may be the access to information regulations applying to the federal government, which allow recovery of reasonable costs from the applicant. Should the law enforcement agency require information of a service provider, which is beyond the normal cost of doing business for that provider, then the agency should underwrite the cost of assistance. The alternative is for providers to raise their subscription rates, thus taxing all subscribers to allow for government action relative to specific investigations. Economic theory would indicate that the users of a good should in general bear the cost of provision of that good, in order to motivate society to rationally allocate effort and costs.

In the section titled "Interception of e-mail", the statement is made:

"..once a communication is put in writing, it can no longer be considered a "private communication" for the purpose of the interception of communications provisions of the *Criminal Code*."

E-mail is replacing paper mail sent by Canada Post and has very similar intellectual attributes. Corporations, indeed, go to extremes to ensure that communications via their internal systems can not be intercepted by third parties. From the point of view of the user, e-mail is much more like a letter than it is a communication. Does not the law with respect to communications intend to differentiate between single channel communications such as the telephone and broadcast communications such as citizens' band radio for the purpose of determination of expectation of privacy? Email is intended to be seen by the sender and recipient, and no other. It would seem that the standards for interception of postal mail

would be appropriate for e-mail. In that context, an ISP's storage systems are analogous to a postal mail bag. An order to intercept e-mail should have equal applicability at any stage of the generation, forwarding, and receipt process.

The final section of the consultation paper deals with problems of identification of subjects. The problem relates to the distributed nature of user directories, whereas there are only a few major telephone companies to contact for telephone subscriber information. A master database of all ISP customers has the potential for abuse. There are countless cases where custodians of address information databases have misused their access and provided mailing lists, etc. In an electronic age, it is not even necessary to maintain a master database. Any database has an associated cost. A better solution would be to keep a much smaller database of service providers, and send specific requests for identification to all. Such requests could be readily automated and authenticated, so that ISPs suffer little overhead for response, yet can be assured that there is proper authority for release of information.

s.19(1)

mailto:

web site:

Kanata, ON

**Pierlot, Paul**

---

s.19(1)

**From:** [REDACTED]  
**Sent:** 2002 Sep 02 10:13 PM  
**To:** la-al@justice.gc.ca  
**Subject:** go screw yourself what will you do next watch people make love in their shithou

fuvk you

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 02 8:41 AM  
**To:** la-al@justice.gc.ca  
**Subject:** Blatant invasion of my Internet accounts

Sirs: I have just read with great concern, the proposal of government to actively monitor my & others communications via the internet. WHY? At the end of the year, government interference in my life, (at every level of government) costs me well over half my income. who is going to pay for this folly?

Government has done nothing to curb the amount of invasive advertising already present, such as pornography, and other stuff like the proliferation of popup advertising, yet you think that reading my email is going to make a difference? Are we on the same planet here?

Before you start creating more regulations, how about enforcing the stuff already in place. You can make all the rules you want, but if they are selectively enforced, (like the present) then they are useless.

I feel the "Potential Terrorist Threat" is just another excuse for government to exercise more control over my life. Gee is it ok if I go potty now?

[REDACTED]

Pierlot, Paul

---

From: [REDACTED]  
Sent: 2002 Sep 02 5:34 AM  
To: la-al@justice.gc.ca  
Subject: Anti-Terrorism Blueprint

s.19(1)

Hello,

I am writing to you in order to ask for details concerning the so-called "blueprint" for our country's new anti-terrorism measures. I am especially concerned that my privacy will be seriously violated if this new bill is passed, after it's introduction later this year.

Any details you could provide would be welcome.

[REDACTED]

Pierlot, Paul

From: [REDACTED] s.19(1)  
Sent: 2002 Sep 03 10:17 PM  
To: la-al@justice.gc.ca  
Subject: Gov't Internet 'Intercept Capability'

RE: Article in the Globe and Mail

On-line spying proposal decried

Ottawa readying law to force providers to let police track customers' activities

By OLIVER MOORE

Tuesday, September 3, 2002 - Print Edition, Page A4

Dear Sirs / Ms'.

Opening mail without a court order is a criminal offence.

It is illegal to tap phone lines without a court order.

These principles are based on the assumption that man is guilty until there is good evidence otherwise. It is also based on the assumption that Canadians are basically good people and don't require that anyone need to monitor their behaviour unless they behave suspiciously. These are assumptions that form significant cornerstones to democratic functioning.

If the principle, authority has the right to monitor what it's wards are doing without prior evidence of possible wrongdoing, then I, as a parent can now sneak into my kids room to check his drawers for potential drugs, even though I have a great kid. As a school administrator, I could check lockers without due cause. As a police officer..... As a .....

In other words, the principle, once accepted as a way of doing business, open a mind set that runs counter to not only who we, as Canadians truly are, but to who we want to be, and who we will become if we betray trust with each other.

Please think twice. I know there are good reasons and arguments for tracking. Yet, there are equally, if not more powerful reasons to counter such a move. At least, wait a little and watch. If the US / Bush aggressive stances fail, as they well might, public backlash against the erosion of national human rights to support government agendas rather than true national well being may significant. If we lose our sense of internal integrity, if we lose our strong sense of identity as a good people, we may become the new negative, suspicious vision of us. The psychology that applies to individuals tends to translate into social principles as well.

Wait also because if you don't, and it goes wrong - well, when was the last time a law was repealed quickly and easily? And it can go wrong.

Thank you for taking the time to read and listen.



Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Sep 03 8:53 PM  
To: la-al@justice.gc.ca  
Cc: Catterall.M@parl.gc.ca  
Subject: "Lawful Access"

Dear Minister Micheal Cauchon,

I wish to file a comment on your ministry's proposed "Lawful Access".

I, like many Canadians, have concerns relating to the monitoring of email/Internet activity by individuals, many of which are not law enforcement officers, who simply perceive criminal activity or intent to perform a criminal act from information they've accessed without just cause. The possibility of misinterpretation cannot be ignored simply because this technology is being used by a severe minority of criminals, whose activities off the Internet would likely be sufficient to gain warrants and convictions without any undue legislation of the Internet.

Another major concern that you will encounter is the financial burdens associated to these proposals to Internet Providers and their customers. Who will eventually pay for the creation of these security measures, the taxpayers or the customers via their Internet providers? And will these security measures reduce the speed of the Internet in any way?

Many Canadians will also wonder how encrypted communications, communications in which "a reasonable expectation of privacy is expected", would be addressed - Will they be by default considered "suspicious" by the security measures and will these be delayed in any way because they are deemed suspicious? And will the security of these communications be compromised in any way, in the name of security? Technologies can differ from one system to another, an attempt to harmonise these systems possibly resulting in hazards that result in a universally vulnerable system.

I believe minor alterations could be made to strengthen our criminal code but crimes should not be isolated or specialised unless the criminal activity can only be found or performed on the Internet. The Internet should be included as a medium on which illegal acts can be performed but fraud is in no way different than Internet fraud and the illegal distribution of material on the Internet is in no way different than that of the same material on another medium. The Internet has facilitated some criminal activities but the Internet should not be inconvenienced or burdened because some criminals saw fit to use this technology to continue their off-line activities online.

I believe that most criminal activities on the Internet could be addressed by amendments to our criminal code resulting in the following:

(1) A penalty up to \$50,000 for all individuals convicted of a crime involving the Internet, collected to compensate any Internet provider whose services were used to perform this activity.

(2) An access restriction resulting in a convicted criminal being unable to access the Internet for five to ten years (as a term of their parole) if the Internet was used to perform a crime.

(3) A penalty of \$5000 for all individuals who use falsified information to gain access to a Canadian Internet Providers services. The term "falsified information" would be defined as "personal information that is intentionally

incorrect or deceiving".

(4) A penalty of \$500 for all individuals who use falsified information in communications of a commercial nature on the Internet, per communication. The term "communications of a commercial nature" would be defined as "any communication that solicits funds for a service, product, charity or investment scheme".

The Internet is so vast that your ministry's proposed system would still likely result in a limited number of interceptions. This proposed system will obviously also meet with some legitimate resistance, this causing delays like that described in your ministry's reasons for the implementation of such a system. This is why I believe it is preferable to police the Internet using complaints obtained from a central, national system established by the RCMP, where individuals and businesses can file complaints (with optional anonymity).

I also believe the RCMP, or a central authority, should gain jurisdiction on Internet crime because it is an international system that reaches beyond any municipal or provincial jurisdiction. I believe some provincial and municipal law enforcement agencies may not be equipped to properly investigate many Internet crimes and the resulting duplication only complicates matters, resulting in incompatibilities within law enforcement itself.

I cannot agree with your ministry's proposals but I do believe some action is necessary. I hope your ministry will alter the proposals in accordance to the public's concerns.

Thank You,

[REDACTED] (Ottawa, Canada)

s.19(1)

- End Of Transmission - No Unsolicited Commercial Email ! -  
- [REDACTED] -  
- The Canadian Music Source Listings -

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 5:07 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Afraid

As a 60+ year old Canadian, when I leave the house to do anything, the chances of me being harassed by the legal system is at least 10,000 times more than being harassed by a criminal or somebody with criminal intent.

I no longer feel even remotely safe in Canada, because the legal system has become so heavily weighted on corrupt law enforcement departments and a seemingly uncaring justice system in the courts.

Now you want to read my emails before I do, well why not just have all emails or web content go to you first and then you could forward what you feel I need to know, then there would be no need for such heavy handed laws like your new upcoming "Lawful Access Laws"

Quote from the Globe..

"The one line that worries me, 'A preservation order ... requires service providers ... to store and save existing data.' Does that mean data that they've already been tracking? It's the words 'existing data' that really and truly bother me." [end of quote]

I am glad I am almost near the end of my useful life as I see Canada sliding down the slippery slope of a Gestapo Government and a Police State. I would rather have some element of crime if it means giving up each and every freedom, a Canadian has expected in the past.

[REDACTED]  
Keswick, Ontario

**Pierlot, Paul**

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 3:37 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Questions and Comments: Lawful Access – Consultation Document

I have a number of questions that are not answered in the Consultation Paper.

1. A question on the numbers of independent companies involved in section:

Legislative Proposals  
Infrastructure Capability  
Requirement to Ensure Intercept Capability

"It is proposed that all service providers ..."

Request #1: In order to make sense of this requirement, please provide estimates or actual counts of service providers of all types.

I believe it is not possible to make a simple extrapolation from intercept mechanisms provided in the past by wireline operators, of whom there were relatively few, to current service providers, of whom there are many. Any decision on this level must be in part based on cost.

Request #2: Could you also provide a count of the number of companies that provide second level connections. That is, companies to which first level service providers connect for access to the internet.

For example, the following section

Issues to be considered

1. how could regulations prescribe technical and other standards or requirements for:

...  
3. the competence, reliability and deployment of employees?

If the conditions on first level providers are too onerous they would prevent the development of small service providers in rural locations. In fact, onerous conditions could drive all small service providers out of business, eliminating the prime source of innovation, training, and entrepreneurial spirit in the internet industry.

2. A request for further explanation of Forbearance.

The section

Legislative Proposals  
Forbearance

is unclear to me. Could you provide additional cases in which Forbearance would apply and situations in which it would NOT apply.

3. The legal distinctions made in

Legislative Proposals  
Amendments to the Criminal Code and other statutes  
Interception of e-mail

are counterproductive.

All government laws should be written in language that treats email at any point in its transmission path as equally interceptable. A reduction of technical detail, which only allows lawyers and judges to make silly argument and decisions, is preferred.

Once an email has been sent by the originator of the message (that step of the protocol, used between user and service provider, that indicates that the send operation is complete has occurred), interception should be possible. To guard against changes to ISP software that would render this definition invalid, the law should require that the communication protocol have such a step and that the step precede any forwarding of any part of the email message by the service provider.

#### 4. Further explanation please.

##### Legislative Proposals

Other mechanisms to provide subscriber and service provider information

This section states that "Determining the local service provider identification (LSPID) information is the first step in identifying a subscriber ...".

What information would law enforcement have to use as a KEY into a database of subscriber location information?

How would it have obtained that information?

I appreciate the catch 22 situation - without knowing who the person is it is not possible to get a warrant to find out who the person is.

However, assuming law enforcement has obtained the KEY legally, then extending a search by using that KEY in a legal database should not be unrestricted. Such unrestricted use appears to assume that all people communicating with a person already under a search warrant are also participating in activities which should subject them to surveillance.

#### 5. Open Source

First a particular example.

All uses of keys into a database that provides personal information which can be used to obtain surveillance permission must be tracked, with that tracking information preserved for future examination by proper authorities to ensure that only appropriate access is made. The systems that provide this database facility should be open source, to allow the wider internet community to prove to itself and the public that the system is not allowing any unauthorized access.

The general principle.

All software that is installed in any part of the internet for use in surveillance must be open source. The public should be assured that only legal surveillance is taking place and it can only be assured by being given full access to the source of the systems used to provide this access.

Victoria, BC, CA

s.19(1)

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 03 3:41 PM  
**To:** la-al@justice.gc.ca

s.19(1)

I for one seriously hope somebody stops this from happening.

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 03 3:33 PM  
**To:** la-al@justice.gc.ca  
**Subject:** IPS surveillance

Government interference in personal privacy issues is a crime against community of the same magnitude as that which they are allegedly seeking to counter. We will never know where they will stop. Our financial transactions would all be vulnerable. Government interference always financially hurts the little guy. My advice is to butt out and spend a little work resolving the issue another way. Be more creative and less invasive.

[REDACTED] s.19(1)

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Sep 03 3:15 PM  
To: la-al@justice.gc.ca  
Subject: BIG BROTHER



Is Canada to become another North Korea or China?

Our National Anthem contains (ed) the words "true north strong and FREE". Methinks that will have to be changed. We are certainly not strong any more and we are rapidly losing our freedom.

I suggest that there be due pause and consideration before any legislation to monitor the internet is made into law.

Sincerely,

[REDACTED]

Stratford Ont.



**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 03 1:39 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Comment on review of lawful access laws

Dear Big Brother,

You deserve no right to lawful access. I pay my ISP for their services, not for policing. These are private sector businesses which control this communication vehicle. Until the you choose to control all ISPs through ownership, you have no right to know where I go and who I talk to using the internet. If you do, I will no longer go online.

Your proposed solution will increase ISP service costs, which will no doubt be passed along to me. Not to mention the increased government staffing and other resources required to administer this legislative change. Thanks but I am already overtaxed and pay too much for internet access.

There are less invasive solutions for fighting crime. You should use this technology in order to setup sting operation websites yourselves. I'm not even trying and I've already given you a simple, targeted solution. If you put any thought into this, I'm sure you could do better than to further limit public freedoms. Your Orwellian solution should only be considered as the last option.

Lawful access is too large of a price to pay for the little benefit it will produce.

[REDACTED] Mississauga ON s.19(1)

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 03 12:48 PM  
**To:** la-al@justice.gc.ca  
**Subject:** "Where" is your web-site?

I tried [www.justice.gc.ca](http://www.justice.gc.ca). I am particularly interested in the discussion paper, posted there, that concerns a law that may require Internet Service Providers to retain traffic logs for six months.

Where might I find this page?  
Thank you,

[REDACTED] s.19(1)

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 03 1:13 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Law requiring ISPs to track their customers' Internet usage

Is this a democratic society or is it communism?

If the government past a law requiring ISPs to track their customers' Internet usage what will be next? What other activities will be tracked?

Tracking users on the Internet is not the answer to the problem of a few people using technology and the Internet to perform scrupulous activities because the majority of people will suffer and their privacy invaded because of a few bad people.

I think the answer is better security and data protection on the Internet.

Tracking users on the Internet is just one more step towards a communist/totalitarian society.

[REDACTED] s.19(1)

Credit Union Central of Ontario  
2810 Matheson Blvd. East  
Toronto, Ontario  
L4W 4X7

[REDACTED]  
905-238-9400

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 11:18 AM  
**To:** la-al@justice.gc.ca  
**Subject:** Access to Internet Information Proposal

Viewing the information released recently, on the Access to Internet Information Proposal I think its a good idea.

A little LARGE however.

**Recommendations**

- 1) Increase law enforcements rights for wire tap to include all media pertaining to the individual. Will cover other types of new media and also quickly swapped cell phones.
- 2) Tech is ready, no problem.
- 3) Only cost is who backs up their files. Put in a caveat on copy instructions and frequency of copy of users data. Also frequency to be delivered to law enforce enforcement. May just want a mirrow sent to the police.

Have a great day..

[REDACTED]

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 03 12:45 PM  
**To:** la-al@justice.gc.ca  
**Subject:** NO

**What is this? Is Canada copying war-time Germany and becoming a police state. A BIG NO to that.**

[REDACTED] s.19(1)

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 10:47 AM  
**To:** la-al@justice.gc.ca  
**Subject:** new proposed legislation

Hi,

I hope the new legislation on internet evesdropping will require the same legalities that a wire tap does. Our society must respect privacy issues.

Regards,

mailto: [REDACTED]

[REDACTED]  
REGINA, SK  
[REDACTED]

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 9:50 AM  
**To:** la-al@justice.gc.ca  
**Cc:** ddimmel@sympatico.ca  
**Subject:** Spying on Internet customers??

To whom it may concern,

I would endorse such a bill only if it needed a warrant first. We cannot endorse a bill with such a high chance of misuse. By implementing this bill you are taking away from Canada as being a free society. Picture this bill being passed: I ask you, what is next? Are you going to force citizens to install GPS equipment in their cars to stop red light runners and other minor traffic offences? This bill is at its best "ludicrous". You cannot punish society because there are others that abuse the internet. We need to set an example for other countries to follow. We are a free society, we are not communists!! This bill is no different than putting electronic tracking bracelets on criminals that have just been released from jail. Oh wait, there is a difference, we're not criminals. Education is the key to all the issues that derive from the internet. Government sponsored commercials telling people why "software piracy is wrong" or other serious offences that take place over the internet. Perhaps this bill would be best implemented on citizens with criminal records. Not on the general society though. Please give serious thought to this bill.

Sincerely,

[REDACTED]

Pierlot, Paul

---

From: [REDACTED] s.19(1)  
Sent: 2002 Sep 03 9:18 AM  
To: la-al@justice.gc.ca  
Subject: Review of Lawful Access Legal Framework

Hey,

I've got a great idea. Why don't you launch a national firearm  
registration authority?

Oh hell, I forgot. You've already wasted that money ...

Marching in the desert...

[REDACTED]



**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 7:50 AM  
**To:** la-al@justice.gc.ca  
**Subject:** New Legislation for access to ISP data

Before considering a reduction in the amount of 'due process' required by investigators to access bank, phone and ISP data about citizens who have not been shown to be guilty of a crime, please consider that you are trading away individual's rights to privacy for security, and allowing the possibility for abuse by investigators in the process. I hope that such a decision can be substantiated by actual hard facts and statistics, and not the heresay and conjecture which seems to be the primary content of the CISC 2002 report - which incidentally seems extremely similar to the reports of the previous two years.

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 2:19 AM  
**To:** la-al@justice.gc.ca  
**Subject:** "Lawful Access", no thanks

Hello,

I am writing as a concerned Canadian citizen to say that I heartily disapprove of the changes to Canadian law proposed in the document at <[http://www.canada.justice.gc.ca/en/cons/la\\_al/](http://www.canada.justice.gc.ca/en/cons/la_al/)>. It trods on my privacy and seems poorly thought-out.

[REDACTED]  
Scarborough ON

[REDACTED]  
Canada

**Pierlot, Paul**

---

**From:**  
**Sent:**  
**To:**

2002 Sep 03 10:07 AM  
la-al@justice.gc.ca

s.19(1)

I do not believe that others should have access to email, it is a form of mail that should remain confidential to the receiver.  
Thank you for your attention

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 06 9:20 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Invasion of Privacy re Internet

s.19(1)

I value my privacy and do not think ISPs  
should have to collect and submit personal  
information about me to the government.  
I also do not think they should use the  
Internet as a means.

[REDACTED]

Pierlot, Paul

---

From: [REDACTED]  
Sent: 2002 Sep 04 10:18 PM  
To: la-al@justice.gc.ca  
Subject: laws

s.19(1)

All I can say is I am against this. I came from a Communist country where they planted bugs in our phones. If you want to do the same thing that would be not Canadian, we risked our lives to come here you know.

Keep our freedom, don't give in to terrorists. Who cares about them. Don't let them take away our civil liberties.

**Pierlot, Paul**

---

From: [REDACTED]  
Sent: 2002 Sep 04 8:49 AM  
To: la-al@justice.gc.ca  
Subject: Cybercrime Treaty

s.19(1)

I cannot believe that a "free" land like Canada is actually considering adopting the Council Of Europe's "Cybercrime Treaty" as it has so far been defined. I am outraged as a Canadian citizen that our government thinks that this is in the best interest of it's people.

I will be finding out who is backing this in our government, and I WILL back those who are against them.

If you could send me more information on this treaty as it pertains to Canada's potential adoption, I would very much appreciate it.

[REDACTED]

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 04 5:22 PM  
**To:** la-al@justice.gc.ca  
**Subject:** RE: privacy and terrorism

s.19(1)

I do not believe that we need to create a state where Big Brother is the norm in every home. The current discussion paper would allow the government and its agents to completely invade the home. The home is the personal and private space of the owners. The discussion paper seeks to give anti-terrorist forces the tools to prevent terrorism. Yet it goes too far. By treating every person, citizen or not, present in Canada, as guilty and requiring supervision greater than that currently used in penal institutions, is not the way to combat terrorism. The discussion paper addresses internet, but sets legal precedents for all forms of communication. As technology is rapidly evolving, and interactive TV is already being experimented with, this can mean watching, listening, as well as monitoring surfing and e-mail. What distinguishes an e-mail from mail sent via post?

I believe that if the government proceeds in the current knee jerk over reaction it will produce an upsurge of resentment and revolution which would make terrorists lives simpler, and policing impossible.

[REDACTED]

## Ministerial Correspondence Unit

From: Web Administrator  
Sent: 2002-09-04 10:39 AM  
To: Ministerial Correspondence Unit  
Subject: FW: Lawful Access – Consultation Document

P02-019038  
MCUED2

Hello,

This letter is addressed to the Minister.

150017

Regards,

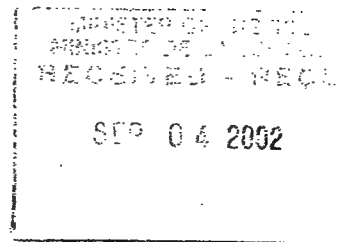
Web Administrator  
Justice Canada  
-----Original Message-----

s.19(1)

From: [REDACTED]  
Sent: 2002 Sep 03 2:59 PM  
To: webadmin@justice.gc.ca  
Subject: Lawful Access – Consultation Document

[REDACTED]  
Merrickville, Ontario  
[REDACTED]

The Honourable Martin Cauchon  
Minister of Justice and Attorney General of Canada  
284 Wellington Street  
Ottawa, Ontario K1A 0H8



Dear Mr. Cauchon,

I have recently heard of the Lawful Access – Consultation Document issue in discussion, and I have to say that I am appalled.

It is inconceivable to me that we now live in a time when ordinary people can have their phones tapped, mail opened and e-mail accessed.

Does no one see the similarities to Nazi Germany?

And now that the US has considered the "family spy network", can we be far behind with an analogous foolish scheme?

Tell me one other thing, Mr. Cauchon, has there been any escalation (and I do mean escalation!) in spys within our borders, terrorism, murder, mayhem ... anything at all ... that would warrant such an assault on our privacy? These problems have always been there and if considered very carefully, I think you will agree that the internet is NOT used by these people to plan their capers. It is used by ordinary citizens every day.

I put it to you that you should ASK Canadians how they feel about such a policy. This is a law that should never see the light of day.

Sincerely,  
[REDACTED]



Ministerial Correspondence Unit / Unité de la Correspondence Ministérielle  
Routing Slip / Feuille de controle

Letter/Lettre Date: 2002-09-03

s.19(1)

Author/  
Auteur:



Document: 2002-019038

Doc Type/Type de Doc: R D

File / Classer: 150017  
LAW - POLICE

Referred To/Transmis a: MCUED2

Date: 2002-09-12

Due Date/Date d'échéance: 2002-10-10

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

Additional Comments / Remarques additionnelles:

YD Regular.  
CLP: CJ- CLP. AH. Lila Lafleur  
Sept 13.02  
α.

CC:  
CC:

CC:  
CC:

CC:  
CC:

CC:  
CC:

Closed / Fermer:

File Away / Classer:

Description of type / Description des types

D: yellow docket / dossier jaune (draft response / projet de réponse)

Further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

Follow-up at your discretion / donner suite à votre discrétion

For your information (no action required) / à titre d'information (aucune mesure requise)

Pierlot, Paul

---

From: [REDACTED]  
Sent: 2002 Sep 04 12:25 AM  
To: la-al@justice.gc.ca  
Subject: internet

s.19(1)

Dear sir

The internet is the only thing in the world and especially in canada that is not regulated to death with idiotic or dummer rules made up by people who have absolutly no idea of what it is like in the real world. If the lawyers are looking for a make work project why not look at the existing laws with an eye to eliminating about 75% of them.

[REDACTED]

**Cloutier, Marie**

**From:** Pierlot, Paul  
**Sent:** 2002 Sep 05 3:54 PM  
**To:** Cloutier, Marie  
**Subject:** FW: Lawful Access Consultation Document

Please file under "other email". Thank you!

-----Original Message-----

**From:** Rule, Jeanette  
**Sent:** 2002 Sep 04 9:59 AM  
**To:** Pierlot, Paul; Angers, Lucie  
**Subject:** FW: Lawful Access Consultation Document

Here is another one that came through the Web Administrator...

-----Original Message-----

**From:** Web Administrator  
**Sent:** 2002 Sep 04 9:54 AM  
**To:** Rule, Jeanette  
**Subject:** FW: Lawful Access Consultation Document

FYI

-----Original Message-----

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 03 8:42 PM  
**To:** webadmin@justice.gc.ca  
**Subject:** Lawful Access Consultation Document

Hello,

I've recently reviewed the proposals of the Lawful Access - Consultation document. I have very serious concern that this goes far beyond what is necessary to insure Canadian safety.

Specifically, the Preservation Order requiring service providers to store and save existing data. This is tantamount to photo copying every letter I send, video taping every move I make, and recording every phone conversation I engage in, all for future review. This is not an acceptable operating procedure by our society's standards. It is clear to me that Law Makers are completely oblivious to what kind of data is actually traveling across Canadian networks. How is long distance voice communication or video conferencing over the internet any different from the same communications carried by a phone line? Unintentionally moving Canada further towards the practices of police state countries by such broad generalizations still results in my rights as a citizen being diminished.

There are other serious problems with the Preservation Order on top of the concerns of its invasion of privacy. The cost to Service Providers to implement such a system will be enormous, as the quantity of data traveling across Canadian networks is staggering. It is easy to foresee that small service providers will have no hope of complying, and that large service providers will simply pass the enormous costs onto the consumer.

Additionally, what occurs when the security on this stored data is compromised? I shudder at the thought of undetected access by the very criminals this is supposed to be protecting us from. (remember, the majority of security breaches occur from within a network, not from external sources).

Sincerely,

---

Chat with friends online, try MSN Messenger: <http://messenger.msn.com>

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Sep 05 1:07 PM  
To: la-al@justice.gc.ca  
Subject: Remarks concerning "Lawful Access - Consultation Document"

I have recently received and read a copy of "Lawful Access - Consultation Document". In general, this is a well thought out document that proposes changes that are long overdue in Canada.

I do have some recommendations concerning the section "Legislative Proposals / Infrastructure Capability / Intercept Capability".

The premise of this section is to require all electronic communications service providers to provide capability for intercepting communications in their network. Specifically targetted are wireless, wireline and Internet Providers.

My concern is with the requirement for Internet Providers. While it seems reasonable that ISPs be required to provide access to the communications that pass through them, the reality is that ISPs are not likely to be technically able to comply in all cases. The exact number of cases that they will be able to comply in is likely to decrease dramatically over the next decade as well as a result of steadily increasing end point security capabilities.

The technical issue is that, unlike wireless and wireline communication providers, ISPs offer "partial transport" and "partial application" services. That is, they typically only provide one segment of service in a typical communication link. Even more importantly, the end points of any link are \*always\* under the control of users or other services -- neither of which is likely to be inclined to disclosure. Therefore, the end points will arrange for security and protection mechanisms that are negotiated and controlled by the end points. The ISP intermediary will have no ability to intercept, interpret, eavesdrop or even provide information about the end points themselves in a such a situation. The best they can do is provide the raw protected data. To require more than that will be cost prohibitive and would see the end of the ISP.

One can ask "what can be done then".

An option is to require that all end-to-end communication not be secured in such a way as to prevent legal access. This concept has been repeatedly discussed and dismissed because it is both technically and economically flawed. The technical flaw is that is that weakening the security to provide lawful access weakens the overall security to the point where it is no longer useful. The economic flaw is that there are classes of communication that it is in the best interests of everyone to be secured as tightly as possible: Financial transactions for example. The type of financial transactions that my company provides software to banks for: ATM transfers, credit card, debit card and point of sale. Many of these transactions run over Internet connected devices these days and they \*must\* be secure. It may be that compliance would force such transactions off the Internet to privately run networks (and associated protocols) to comply, but at huge economic cost.

The bottom line is that, as far as the Internet goes, it will be very hard to restrict or require the transport service provider with a lawful access order. They will not be able to comply in all cases. In fact, the

data that ISP's do have today in the form of applications and application data is likely to disappear over time. The economics of running an ISP place applications like email and web services clearly on the "cost only" side of the equation and they are likely to disappear.

You have to go after the endpoints. I believe that you already have the solution to this in the form of the production orders. In particular the production orders need to include all of the following:

- Original document/data
- Security Keys
- Protected document/data

In this way, you can acquire content via ISPs that can then be used to verify transmission of documents/data as part of a committing a crime.

The downside is that such an approach is purely reaction oriented and provides no capability for intelligence gathering or preemptive law enforcement. This is unfortunate.

I can offer no real alternative to the intercept proposal for ISPs. I have no doubt that it will work partially and in the beginning in some percentage of cases. Regrettably, I think that it won't be good at catching the instances that need to be caught and it has the potential to place an economic burden that jeopardizes an already weak commercial ISP industry segment.

Much will depend on how the details of the requirement and level of technical reality in the compliance order.

Cheers

s.19(1)

ACI Worldwide

The largest single provider of secure financial transaction software in the world.

"Every Second, Every Day"

Email:

Phone:

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 07 1:06 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Privacy of email and phone conversations

There is no excuse or rationalization that can ever make it acceptable  
for the State or monitor my email communications!

[REDACTED]  
Qualicum Beach BC  
The Fascist Dictatorship of Canada,  
A sleazy Component of the Corporate Fourth Reich

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 07 4:12 PM  
**To:** la-al  
**Subject:** Odd Email Message Dated 29/08/02

Please allow me to first apologize for the stupidity you were forced to read. I have had a security hack of my own to deal with, in the form of a fool who was visiting me. That person will not be allowed to have computer access here any longer. I found out about this little escapade when I happened to drop past my computer and checked the logs and outgoing mails. I have been sending apologies near and far. Please disregard this message, though I am sure that you would have every right to be upset. I have read this email, and I have talked with the person and found out about other transgressions using my computer in the recent past. I apologize to any one person or persons who may have been offended by the email in question. I cannot apologize enough.

[REDACTED] s.19(1)

Halifax, NS.

[REDACTED]



**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 08 7:20 PM  
**To:** la-al@justice.gc.ca  
**Subject:** anonymity s.19(1)

I don't think the proposed draft should be passed. The government and the police already have laws that can catch a criminal on line. The individual person should not be penalized for what some may do. The individual should be able to maintain anonymity on line.

[REDACTED]

Cloutier, Marie

---

From: [REDACTED] s.19(1)  
Sent: 2002 Sep 08 2:59 PM  
o: la-al@justice.gc.ca  
Subject: Comments about - The "Canadian Lawful Access" Legislation

While I agree we need some sort of gov't involvement. We must make sure that external treaties do not violate our constitution and Charter.

Monitoring of internet traffic is a tricky issue. Certain things online should be monitored. But I disagree that email, web usage should be monitored nor access to remote systems.

This law seems to think ISPs are the only ones who handle internet services. This is not true. Many users can run their own mail servers. Does that mean I have to keep records of my own email? That's pretty stupid to me. Just because I run a http/httpsd/smtp/pop3 and dns services does \*NOT\* make me a "service provider" when I'm only providing service for myself! (excluding DNS/web)

I don't feel the Law community has enough technical understanding on how the internet works nor how technology is in general. Before passing laws it should get a better understanding of technology and the internet before draconian laws like the DMCA etc are passed in Canada.

Thank you,

[REDACTED]

Pierlot, Paul

From: [REDACTED] s.19(1)  
Sent: 2002 Sep 08 5:21 PM  
To: la-al@justice.gc.ca  
Subject: consultation on ISP-assisted police spying

I understand the government wants to know what Canadian citizens think on this issue. I understand the issues, technical and political, and hope that you will read my reasoning, below the brief opinion.

1. should Canadian ISPs be legally obliged to have the technical capability to keep a record of an individual's Web surfing and email history upon request?

No. This is invasive and unnecessary.

2. should there be a special provision for email?

Yes. It should be treated like private correspondence or phone calls.

Reasoning:

Until the case is made specifically, made very well, and made publicly, that common police forces require privacy-invading authority that we have thus far denied them, the justice department should *not* expand police powers with regard to Internet communications. There has been no case made that Canadians require or deserve less privacy when communications are digital rather than analog electronics, or indeed when they employ electronics as opposed to pen and ink, and I doubt such a case can be made.

We already permit all but unchecked invasions of privacy by spy forces in the name of national security. ISPs already keep email records for a time, and will keep any records additionally requested by a legal warrant. The electronic nature of these records already modestly advances the ability of both our spy agencies and common police to investigate when compared to prior communications technologies. In requesting more authority, police must be hoping that the government of the day is so technologically dim or cop-complacent that it approves a wider baseless snooping power.

With even a modest understanding of the Internet, it's easy to make appropriate comparisons. E-mail is quite like a private phone call, fax or posted letter, and deserves no more or less privacy. Should police have easy access to a list of people one has e-mailed? Perhaps, but only if a judge would grant them similar access to detailed phone logs, and allow them to intercept the snail-mail carrier in order to log to addresses (but not read the contents of) one's letters. To justify reading one's e-mail, the police should pass a stricter test; the same test as for tapping a phone or opening snail mail.

Web pages that a citizen creates or comments that one posts online are like classified ads or letters to the editor in a print publication. Since these are public, there is no need for permission to view them. But pages viewed are quite different. It is silly for police to require that ISPs keep a log of Web sites each individual has visited, in case they decide to snoop later on. Web pages viewed are like TV shows tuned, magazine pages flipped, or books checked out of the library. We should be very leery of police who say want to investigate—and deem a particular citizen suspicious—based on his or her choice of channels or reading matter, online or offline.

The Web log gambit would inconvenience private companies and bolster police powers with scant hope of solving crimes. So where does this request come from? Internet newbies? Maybe. Perhaps also, in part, from the realm of fiction; that's where cops track a serial killer—who leaves hints of seven deadly sins and an obscure reference to a Dante passage—and find him via an illegal search of books checked out of the library. But I suspect it mainly comes from a well-intentioned desire to

enforce a well-intentioned but faulty law: the anti-child porn act.

Only the most outspoken civil libertarians publicly criticize this kiddie porn law. It's far easier, given the revulsion we feel to those who are fixated on immature or prepubescent boys or girls, to hope that few undeserving people will be caught breaking the overly broad law, or at least that this will be outweighed by the harm prevented. But that's exchanging something quite precious for a faint hope.

Banning repulsive images and ideas, rather than just outlawing harmful deeds, treads across the line that protects precious democratic rights. Sure, the world might be a better place if there was no kiddie porn, online or otherwise. That won't happen, but perhaps it would be a slightly better place if only Canada's little corner of the world was somewhat cleaner. And perhaps people can distinguish between Nabokov, Mapplethorpe and "barnyard fun" Web sites that, e-mailed spam claims, feature "donkeys and lolitas."

But even if you believe that police and judges will reliably separate these (I don't), the law is an ass. Speech should be free, unless it externalizes its cost to the recipient, like spam or junk faxes. Speech *only* needs to be protected *when*—not *until*—it offends. Outlawing images, ideas and associations is the hallmark of Taliban-style fundamentalist thought, and is the antithesis of liberal democracy. We are supposed to tolerate until someone is harmed, even if this sentiment is less firmly established in Canada than south of the border.

It has long been, quite rightly, illegal to make kiddie porn or to perform sexual acts with minors. And of course those guilty of these harmful crimes deserve prosecution to the full extent of the law, though this can be done without the kiddie porn law. But in the Internet age, untold thousands of men who would never sexually touch a child have likely once seen such an image of a minor. They, and even citizens who view kiddie porn sites only to report them to police, have broken the law.

Few would baldly call for most citizens to be casually stripped of their freedoms by the state, the police, or the courts because the odd one is a potential deviant or friends with a criminal, yet this is exactly the implication of the kiddie porn law. Decades after we wrested the library acquisition lists from church prudes and got the state out of the bedroom, we have inviting them to monitor our communications and snoop on those it finds to have prurient interests.

Perhaps by criminalizing the many, we have enabled cops to catch a few who have or would hurt a child. But even if police only ever charge kiddie porn fanatics, some of who might act on their urges, a law that can convict people for thought crimes is illogical, lazy and backward. Like banning *Lolita* from libraries to condemn pedophilia, branding someone a commie merely for reading Karl Marx, or labeling them a Nazi for watching the Third Reich-obsessed History Channel, it is wrong even if it may at times hit the mark.

Even if well intentioned or popular, bad laws should be resisted, starting with this Orwellian proposal to track all Web sites that each Canadian views. This has nothing to do with combating terrorism.

Even the most charitable explanation is that it will ease enforcement of a thought-crime law. If ordinary people or politicians were brave enough to critique such laws, this odious idea would be dismissed as soon as a cop or suburban alarmist first proposed it. That it wasn't should give us all pause.

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Sep 08 7:19 PM  
To: la-al@justice.gc.ca  
Cc: cips-security-sig@interchange.ubc.ca  
Subject: "Lawful Access" Consultation document

s.19(1)

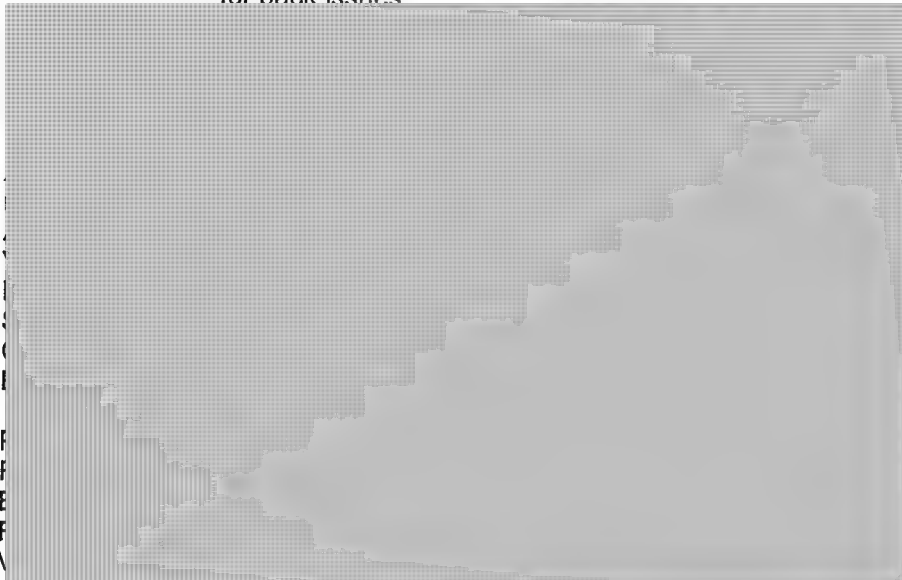
I note, in regard to the document that starts out "Several amendments to the Criminal Code have been proposed to deal with the interception and search-and-seizure provisions noted above, and to permit Canada to ratify the Council of Europe Convention on Cyber-Crime" that a section is labelled "Virus Dissemination."

Of concern is that sentence that states: "The Council of Europe Convention on Cyber-Crime requires signatory states to criminalize the creation, sale and possession without right of devices (e.g., computer programs) that are designed or primarily adapted for the purpose of committing offences specified in the Convention, whether or not the virus has been deployed or has caused any form of mischief." As a researcher in the field of computer virus programs, I am far from being in support of the writing of viruses, but I should warn you that wording such a section is fraught with peril. Defining a virus, in legal terms and in such a way that it does not include unrelated software, is not an easy task. It is quite possible for such legislation to end up criminalizing utility software such as DISKCOPY, which has been part of DOS and Windows for years.

=====  
"If you do buy a computer, don't turn it on." - [REDACTED]

Guide to Computer Viruses" 0-387-94663-2 800-SPRINGER  
"Viruses Revealed" 0-07-213090-3

=====  
for back issues:



**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**To:** 2002 Sep 08 9:20 AM  
la-al@justice.gc.ca  
**Subject:** Will Canada force ISPs to spy?

To whom it may concern

I am outraged at the notion of my government or its agencies spying on me let alone passing a law that would allow them to do so. I will not stand for this invasion of privacy. I will make my voice heard and my votes count on this issue.

[REDACTED] Moncton, New Brunswick

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 11 10:12 AM  
**To:** la-al@justice.gc.ca  
**Subject:** Protect Canadians privacy from the USA

s.19(1)

First of all I don't want foreign governments including the USA to have the ability to monitor my movements on the internet. Maybe all you politicians think the USA has our best interest at heart My self and allot of other Canadians don't see it that way.

Secondly before any Canadians rights are violated in the name of police enforcement, war on terrorism, etc the law enforcement should have to go in front of a Canadian judge and present evidence that justifies the breach of individuals privacy. This would prevent law enforcement from abusing there authority.

[REDACTED]  
Enterprise Server/Storage Support  
Customer Support Center CTH  
Phone: [REDACTED]  
Fax: [REDACTED]

CANADIAN CABLE TELEVISION ASSOCIATION  
ASSOCIATION CANADIENNE DE TÉLÉVISION PAR CÂBLE

September 13, 2002

Mr. Paul Pierlot  
Senior Advisor  
Lawful Access and Internet Content Policy  
Criminal Law Policy Section, Department of Justice  
East Memorial Building, Room 5024  
284 Wellington Street  
Ottawa, Ontario M4W 1G9

Dear Paul:

The Canadian Cable Television Association (CCTA), the Canadian Association of Internet Providers (CAIP), the Canadian Wireless Telecommunications Association (CWTA) and the Canadian Advanced Technology Alliance (CATAAlliance) have had an opportunity to complete an initial review of the government's Lawful Access Consultation Document, which was released on August 25, 2002.

The technical and legal issues associated with the proposed framework are highly complex and will require extensive consultations with the memberships of our respective associations, including a detailed analysis of the proposals at an operational level. Given the scope of the consultation paper and its potentially significant implications for our members, we are concerned that it will be very difficult to provide a meaningful response by November 15.

To ensure that industry participants are in a position to provide the government with an informed and comprehensive response to the proposal, CCTA, CAIP, CWTA and CATAAlliance request that the deadline for written comments be extended to January 31, 2003.

Yours truly,

s.19(1)

Senior Vice President & General Counsel  
on behalf of CCTA, CAIP, CWTA and CATAAlliance

cc. Michael Binder, Industry Canada  
Allan MacGillivray, Industry Canada



Cloutier, Marie

---

From: [REDACTED] s.19(1)

Sent: 2002 Sep 13 8:44 PM

To: la-al@justice.gc.ca

Subject: lawful access

To whom it may concern:

Forcing ISPs to provide information about their subscribers to law enforcement officials is something that I as a Canadian internet user find abhorrent.

How can this claim of "emerging threats such as cyber-crime" possibly justify this blatant invasion of privacy?

The real experts will be way ahead of any tracking system, so why not concentrate our already overstretched law enforcement resources in areas where they can really make a difference. If someone wants to hack into my computer or defraud me through an email spam, I will take my chances.

What concerns me more is what is going on the streets of our cities and communities, and that requires more we are getting of old fashioned police work.

\* Thank you for considering my opinion.

[REDACTED]

Victoria, BC

2002-10-01

000051

Cloutier, Marie

From: [REDACTED]  
Sent: 2002 Sep 16 4:49 PM  
To: [REDACTED]  
Subject: Lawful Access (Internet Surveillance)  
E-Mail

s.19(1)

I think your paper is unrealistic in some aspects of e-mail. Internet e-mail is not private because of the very nature of the Internet. That is why the only method of securing Internet e-mail is by encrypting it.

Hence:

(1) no court order at all should be needed to intercept and read any e-mail passing through any and all ISPs in Canada. This system is used by the FSB in Russia and I gather that the FBI had a program called Carnivore doing much the same in the USA. There can be no reasonable (underscoring 'reasonable') expectation of privacy where the medium is inherently public. Postcards come to mind as an analogy. Ignorant expectation of privacy is not reasonable expectation of privacy. The class within which the reasonableness is decided is that of moderately informed users, not dummies.

(2) compelling the production of encryption keys or else compelling the decryption of encrypted e-mail by sender or receiver is an invasion of privacy, as the sender and/or receiver has/have indicated that they expect privacy by encrypting the message(s). Hence Court order required.

(3) Installing hardware or software devices on a person's keyboard is also obviously an invasion of privacy, as even if the informed do not expect the state to be reading their keystrokes. Hence Court Order required.

(4) interception and cracking of e-mail by the state is also an invasion of privacy, for the same reason as requiring the provision of keys or requiring the sender or receiver to decrypt the message(s) in question. The agreement between the various English-speaking countries to exchange intercepts/decrypts of each other's nationals is/was an invasion of privacy and an end-run around the restriction on each national agency on surveillance of its own citizens, which was speciously legal at best. If I am not allowed to spy on you but my friend is, I can't ask my friend to spy on you for me: it is an elementary principle of law that one cannot do indirectly what one cannot do directly (in another context, the Margarine Reference and the specious use of the Federal criminal law power comes to mind).

Practical solutions:

(a) set up a system whereby all Internet e-mail is intercepted/interceptable by the state and (where needed) recorded. The stupid criminals will be get caught there.

(b) set up a system for obtaining Court orders for either the surrender of encryption keys or else installation of keyboard sniffers for the brighter criminals;

(c) make sure that state security agencies that intercept and (attempt to) decrypt traffic without the knowledge of the sender/receiver are tightly controlled, with Court orders being needed to (attempt to) decrypt encrypted traffic, and with an annual report to a truly independent watchdog, from whom the intercepting state agency can hold back nothing.

s.19(1)

Toronto, Ontario

20 September 2002

Criminal Law Policy Section - Lawful Access Consultation  
284 Wellington St., 5th Fl,  
Ottawa, Ontario K1A 0H8

Re.: "Lawful Access" legislation

To whom it may concern:

I write to express as a computer professional my concern about the federal government's review of legislation to extend law-enforcement "wiretapping" to the Internet.

The proposed legislation, while not fully described yet, seems to be expanding law enforcement power, without adequate expansion in privacy protections, public "access to information", or judicial and ministerial oversight. While it often sounds like a good idea to expand these powers, it can go too far. The balance between privacy and surveillance by intelligence and law enforcement has evolved over a long period. Fighting terrorism may require new surveillance powers, even extraordinary ones. But each new power comes at a cost, and the cost must be weighed against any benefits.

I think the current balance of power between privacy and "lawful access" is appropriate. I do not feel unsafe, nor have I seen credible, substantial evidence that Canadian people are at risk given the ability of criminals to communicate using the Internet or other electronic media. It may be that, in other countries more threatened by terrorism, the balance needs to shift farther toward surveillance, and away from privacy. But this is Canada, and even if we are threatened more than we realize, the threat is less than in many other places. Thus, ratification of the international treaties, like the Council of Europe Treaty on Cybercrime, is not an adequate motivation for changing our domestic privacy protections. If our allies' law enforcement agencies ask our public courts for subpoenas or search warrants, perhaps via their domestic peers, we can and should help them.

Various courts in the U.S. and Europe have recognized the importance of anonymous speech (especially political speech), affording it constitutional protection. They reason that an identification requirement for speech would tend to restrict the freedom to distribute information, and thereby restrict the freedom of expression. This is important to the speech of political insiders- perhaps people in the government itself, and especially in the political opposition. But our Constitution ought to protect this right for all members of the public.

Here are some of my objections and recommendations for any "Lawful Access" legislation:

1. It imposes an unreasonable **burden on private enterprise**. Companies should not have to do the work of police. They should be free to manage their computer systems

as appropriate for their business. They should have the freedom to design their systems for efficiency, security (including safeguarding customer privacy), and low cost. They should not have to complicate their designs to ease police investigative work. The Justice Department's Consultation Document refers to onerous compliance regimes, which sound like a nightmare for busy engineering staff with better things to do. Security is particularly important. Any access for law enforcement will unquestionably **weaken protections against unlawful access** by criminals inside or outside an Internet provider.

2. When police need to read citizens' e-mail, track online activity, etc. they should go before a public court, argue their case, present evidence, and get a search warrant or subpoena. This is the **due process** of law, guaranteed by the Charter of Rights and Freedoms. I trust the courts to grant access when it is required, and to otherwise withhold it. Police should trust them, too. That setup has a nice side-effect: the media and public can watch what is going on, and raise an alarm if power is being abused, or if, in fact, too many obstacles are being put in the way of expedient law enforcement.
3. Law enforcement should never have direct or real-time electronic access to Internet Service Providers computers or records. This invites "**fishing expeditions**", and weakens the oversight that the courts and Parliament should be exercising. Electronic communication may be fleeting, but once law enforcement gets hold of it, it is particularly easy to **track, sort, and profile**. It's too easy to abuse if access is not checked with due process, and, yes, administrative and resource constraints. If it takes real effort and money, the police will only undertake to snoop when it's truly warranted.
4. Any new legislation should draw a strict line between the **content** of electronic communications, and logs about communications **traffic**. For instance, almost all Internet Providers maintain logs of who sent an e-mail, to whom, and when. Logs of the web pages each customer browses are also kept, and which network ("IP") address to visit those web pages. But these are separate from what was actually on those web pages, or what was actually written in an e-mail. Thus we draw a distinction between *content* and *traffic*.

This so-called traffic data can be made available by subpoena, if the Internet company still has it. Under no circumstances should a provider be compelled in advance to store the actual content of communication. If law enforcement requires content, they should seek a subpoena after presenting to a court evidence that meets an even higher standard than that for traffic data. It is important to note that the *Subject* header of an e-mail, and the *URL* of a web page, should be considered strictly content, and not traffic. Both can contain lots of information beyond the time of and parties to a communication

5. The Consultation Document refers to a potential **nationwide database** of Internet users. Such databases always raise the spectre of terrible abuse of privacy. Compelling service providers to supply data for such a database will likely place the provider in a conflict of interest with its customers. Most of those customers today already demand that they are not listed in directories maintained by their providers, and to protect their privacy in other ways.

In conclusion, I think the status quo, involving court-ordered subpoenas and search warrants, is the best balance between privacy and lawful access. Compelling industry to be complicit with constitutionally questionable wiretapping is costly, and sets a bad precedent of deputizing private enterprise in the enforcement of law. It seems to me that this legislation is being driven by law enforcement interests both inside and outside the federal government, largely as a step in the Canadian ratification on the Council of Europe *Convention on Cyber-Crime*. There seems to be a real lack of involvement by the public, Internet companies, or even parliament. I do not believe we should ratify the Convention.

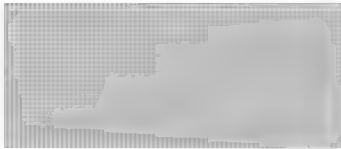
I won't be supporting any government that doesn't defend Canadians' privacy. Law enforcement and intelligence may find that due process of law in public courts, and administrative and constitutional hurdles to eavesdropping are seriously inconvenient. But they are fundamental to democracy, and cannot be given up for long before democracy is weakened.

On the other hand, I would applaud and support (and vote for Members of Parliament supporting!) legislation that

- Protects the privacy of Canadians' use of the internet
- Explicitly recognizes the right to **use the internet and cell phones anonymously**
- Explicitly recognizes the right for public libraries and "Internet Cafés" to offer patrons anonymous Internet access
- Explicitly grants domestic electronic mail the same privacy status as **paper mail**
- Explicitly recognizes the right of Canadians people to use cryptography to keep their communication and records secret, and, consistent with the rights against self-incrimination, to not be compelled to divulge their encryption keys
- Prescribed handling procedures for evidence obtained by wiretapping, including **dual-criminality** provisions governing "sharing" of such evidence with law enforcement or intelligence agencies in foreign countries

Sincerely,

s.19(1)



## Ministerial Correspondence Unit

From: [REDACTED] s.19(1)  
Sent: 2002-09-23 12:13 PM  
To: consultations@canada.justice.gc.ca  
Cc: la-al@canada.justice.gc.ca  
Subject: Comments on "Legal Access Discussion Paper"

THIS ADDRESS IS  
NOT CORRECT, SO IT  
NEVER WAS RECEIVED  
IN THE la-al mailbox

DNL PIELLOT

Dear Sir/Madam:

I am providing my comments with respect to the "Lawful Access Discussion Paper" provided on the Department of Justice website.

I wish to express some extremely serious concerns with, and my objections to, many of the proposals in this discussion paper. Many of the proposals chip (dynamites?) away at the protections afforded the Canadian public.

Further, I wish to express my absolute dismay that this "Discussion Paper" is tilted so far towards the removal of privacy and protections.

My comments follow:

### 1) Infrastructure

All internet service providers ("ISP") would be required to provide, at a minimum, a basic intercept capability before providing new services or a significantly upgraded service to the public.

Why? Do you also expect that when I encrypt documents or email, that I would have to turn over passwords to a third party escrow? I hope not, yet that is the slippery slope that we are going down. Intercept capability shouldn't become a certainty.

Further, Bell Canada doesn't provide tape recorders when police have a warrant to wire tap, nor does Canada Post supply photocopiers when access to

the mails was being similarly provided. I fail to see why ISPs should bear this cost, which would ultimately be pushed down to myself, as a consumer.

This appears to follow along the lines of extremely onerous UK legislation, that raised significant ISP and consumer concerns. I don't like the UK legislation, and I have no wish to see any similar effort in Canada. In fact, given the limited number of search warrants or production orders that might be obtained in Canada (versus the UK) it makes less sense that you require EVERY ISP across Canada to purchase new equipment, when centralised police forces can instead obtain relevant equipment "as need dictates".

Installation of intercept capability at an ISP, also allows the ISP and its employees to more easily monitor my internet use. This would invade my privacy - no offense, but I don't trust my ISP that much!

As a final point, I would point you to such FBI projects as Carnivore, which

provide intercept capability to the FBI, when hooked into an ISP. The ISP does not need to install intercept capability. What your proposal in fact suggests is that Canadian police forces are technologically inferior to those in the US, and that as a result the Canadian public using ISP should foot the bill. No offense, but I'd rather not, especially where the costs

are far greater than providing for a single police unit with proper technological capabilities.

## 2) General Production Orders

The suggestion is that rather than having policing authorities execute a search warrant, a "general" production order could be used to require third parties (such as ISPs, Banks) to produce whatever general information they might have. There would be no entry into, the premises of the third party, and such production orders would also allow law enforcement officials to obtain documents in cases where documents are stored in a foreign country.

I am absolutely opposed to this suggestion. Worse, is the suggestion that the Criminal Code allow "anticipatory" orders. The safeguard is not to in any way effect this suggestion.

I am also VERY concerned by the suggestion that Canada would extend the effect of a judicial order, beyond its borders. It wasn't that many years ago, that Canadian banks in the US were threatened with massive fines if they did not turn over documents from their caribbean subsidiaries.

There are mechanisms and treaties in place to obtain documents in foreign countries through "LAWFUL" methods. Obtaining documents from a foreign country, without means of a search warrant issued by that foreign country, could very well be unlawful. This would subject Canadian 3rd parties who complied with the General Production Order, to fines or other measures by that third party.

Canada must not act in an extra-jurisdictional manner, lest other countries do the same. One United States is enough in the world.

## 3) Specific Production Orders

This proposal would allow a specific production order to be created under a lower standard in order to allow for the production of telecommunications associated data, although not the specific data, or transmission, itself.

The Discussion Paper appears to suggest that routing information for internet traffic, packet sizes, etc. would be the subject of this lowered standard.

No, there should not be a specific power, parallel to that provided for in the Criminal Code for dial number recorders, that would allow law enforcement and national security agencies to obtain traffic data.

As a member of the public, my use of the internet, the traffic routings I take, the web items I view, are far more than just knowledge of a number dialed. This suggestion gives policing authorities carte blanche to determine for instance, what I read on the web. Its more akin to a police officer following a person through a bookstore and looking over their shoulder to see what they are reading. This change would significantly impact an individual's rights to privacy, without the protection of the requirements needed for a search warrant. This is far more than the analogy

of a "telephone number" as suggested, as would, by its nature, provide specific data, ie. the data viewed.

With the internet, there is no distinction between the Domain Name Service number for a web page, or a user/ISP. They can't be differentiated, and as a result, this proposal has no merit, unless we are prepared to allow policing authorities to look over our shoulder at the bookstore. I'm not!

#### 4) Orders to Obtain Subscriber or ISP Information

I have no objection, except if this proposal were to require ISPs to retain information that they might not otherwise retain.

No additional burden should be placed on ISPs, nor should consumers who take steps to guard their personal information or privacy, be thwarted due to government requirements imposed on ISPs

#### 5) Assistance Orders

Yes, assistance orders should more clearly spell out the scope and limits of

what a person may be required to do to give effect to the warrant or authorization, and where legislation already allows for the issuance of search warrants or the granting of interception authorizations, it ought to be amended to include the possibility for a judge or justice to issue an assistance order to give effect to the warrant or authorization.

#### 6) Data Preservation Orders

This item presupposes that a Data Preservation order is a necessity? While it is a procedural mechanism in the Council of Europe Convention on Cyber-Crime, that does not mean that Canada need necessarily adopt a "Preservation Order".

Article 16 states "Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or

similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system" (I'm biting my tongue and not commenting on the idiocy of signing this Convention in the first place - I can only hope it is not ratified in its present state)

Canada already has measures in place - a "search warrant".

If this measure is still required and given an order of this nature is "temporary, remaining in effect only as long as it takes law enforcement agencies to obtain a judicial warrant to seize the data or a production order to deliver the data", then the order should not exceed 30 days. That is enough time to obtain a proper warrant.

A data preservation order could apply to paper or data records, and there should be no penalty applicable other than through contempt of Court proceedings, particularly as there may be exigent circumstances that prevent full compliance.

Orders of this nature should be issued by the Solicitor General's office, and should only be initiated as a result of a request by Competent Authority

under the Council of Europe Convention on Cyber-Crime. Domestic laws should not be extended beyond the barest of minimums to comply.

#### 7) Virus Dissemination

The Criminal Code wording needs to include the concept of "intent" with respect to the creation or possession of a virus. For instance, if I innocently get a virus, I could be in violation of the Criminal Code, and there are a multitude of legitimate reasons security reasons to have virii,



not to mention, an awful lot of computer software can cause damage if used improperly or in the wrong context, yet would not normally be "virii".

### 8) Interception of Email

"private communication" to cover any oral communication, or any telecommunication made under circumstances creating a reasonable expectation of privacy.

I do not buy into the suggestion of the Discussion Paper that this appears to suggest that, once a communication is put in writing, it can no longer be

considered a "private communication" for the purpose of the interception of communications provisions of the Criminal Code.

Rather, there is a broader implication, and the expectations of the parties to the communication are paramount. The Alberta judgement referred to, would tend to confirm that view.

Given the store and forward nature of email communications, I am of the view

that if a specific provision of the Criminal Code is set out to address the issue, then it should do so in favour of the more rigorous requirements of a

"private communication". I view my emails as a private communication, irrespective of the fact that they may end up residing on numerous servers, as they are forwarded through the internet to a recipient.

Varying the type of order to be obtained in order to acquire an e-mail, depending on the stage of the communication or delivery process, is ungainly, and confusing. Further, as expressed above, I personally view any email as a private communication.

### 9) Competition Act - Access to Hidden Records

This item is unclear. Is it proposed that persons would be required to provide passwords to allow policing authorities to break encryption?

If so, what penalties? What if they've forgotten the password?

Worse still, couldn't this implicitly require a person to incriminate themselves and be in violation of paragraph 11(c) of the Charter? I don't see this proposal as having much practical merit.

Yours truly,

[Redacted]  
s.19(1)

Toronto, Ontario  
[Redacted]

---

Chat with friends online, try MSN Messenger: <http://messenger.msn.com>

Ministerial Correspondence Unit / Unité de la Correspondence Ministérielle  
Routing Slip / Feuille de controle

Letter/Lettre Date: 2002-09-24

Author/ Calvin D. Bruner  
Auteur:

Document: 2002-020014

300 Westlake Avenue  
Toronto ON  
M4C 4T6

Doc Type/Type de Doc: **XF**

File / Classer: 150017  
LAW - POLICE

Referred To/Transmis a: **MCUED2**

Date: 2002-09-27

Due Date/Date d'échéance: 2002-10-28

**CLP & CJ-CLP**

Attention: **Catherlyne Boudette**

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

Additional Comments / Remarques additionnelles:

*Def 4/52  
→ Catherlyne  
for action. - if no reply.  
is to be sent, ask Lela  
to record this on her  
system, did*

CC:  
CC:

CC:  
CC:

CC:  
CC:

CC:  
CC:

Closed / Fermer:

File Away / Classer:

Description of type / Description des types

D: yellow docket / dossier jaune (draft response / projet de réponse)

A: further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

Follow-up at your discretion / donner suite à votre discrétion

your information (no action required) / à titre d'information (aucune mesure requise)

September 25, 2002

Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

To whom it may concern:

I read with some interest the "Lawful Access -- Consultation Document", published on August 25, 2002 and would like to submit the following brief comments for your consideration.

I believe the public policy objectives of the proposals laid out in this document, particularly the intention to "update the existing legal framework to help law enforcement and national security agencies address the challenges posed by advanced communications and information technologies", are sound, provided these are done within the guidelines established by the Charter of Rights and Freedoms.

I also generally agree with the proposal to require wireless, wire line, and Internet service providers to provision their networks to permit lawful access to national security and law enforcement agencies. This will help simplify the legal framework for communications interception by unifying disparate intercept provisions for wireless personal communication services (as stated in the Radiocommunications Act), older wire line (or "plain old telephone service") networks and internet protocol (IP) networks.

However, the implementation of the requirement that signatories to the Council of Europe's Convention on Cyber-Crime criminalize the "creation, sale, and possession without right of devices (e.g., computer programs) that are designed or primarily adapted for the purpose of committing offenses specified in the Convention" should be deliberated carefully, in order not to inhibit the academic study of computer virus or the commercial development of anti-viral software products. Criminal intent should remain the standard by which prosecution is undertaken, and not mere possession. With few exceptions, viruses infect and reside upon systems without the consent and knowledge of the operator, owner, or administrator. A proper definition of what constitutes a computer virus must also be established so as to not inhibit the legitimate development of software products (for example, autonomous software agents) with characteristics similar to viruses (self-replication and mobility).

With regards to the proposal that service providers be required to log network transactions (mail and web access, for example), the following should be considered: mail and web logs are

voluminous and a legislative or legal requirement to maintain them for long periods of time would impose onerous storage hardware costs upon service providers. In particular, this may pose a problem for smaller community or family operated internet service providers (ISP) which often operate at small profit margins in a very competitive market.

Finally, the proposal to create a registry of internet service subscribers or users is unrealistic, considering the multitude of consumer devices (personal computers, PDAs, cellular telephones) via various connection media (cable, DSL, wireless, telephone dial-up) that now provide access to the internet. How will the anonymity often afforded by these devices be addressed? Will the instant obsolescence of a subscriber registry through the churn of provider accounts be taken into account? And thirdly, how well will such a system function, considering the tremendous amount of coordination that will be required in order for a centralized database to be created and maintained? Will the benefits gained justify the cost of this endeavour?

I would propose that if a mechanism for gathering Customer Name and Address information (CNA) or Local Service Provider Information (LSPID) is necessary, individual service providers perhaps should be under a legal requirement to acquire and maintain current subscriber information. This would provide law enforcement and security agencies the means by which they could identify criminal actors, while eliminating the privacy concerns that a centralized database raise. It would also be more cost effective for the service provider to absorb the incremental expense of tracking each subscriber, than what will be incurred by the public agency responsible for the establishment and maintenance of a centralized registry.

Sincerely,

s.19(1)

Delta, B.C.

Cloutier, Marie

s.19(1)

From: [REDACTED]  
Sent: 2002 Sep 25 4:57 PM  
To: la-al@justice.gc.ca  
Subject: Fw: Privacy

----- Original Message -----

From: [REDACTED]  
To: <laal@justice.gc.ca>  
Sent: Wednesday, September 25, 2002 1:47 PM  
Subject: Fw: Privacy

>  
> ----- Original Message -----  
> From: [REDACTED]  
> To: <laal@justice.gc.ca>  
> Sent: Wednesday, September 25, 2002 1:30 PM  
> Subject: Privacy  
>  
>  
> I am responding to the following information which I received in an email.  
> I would like to express my concern and dismay at this proposal. Email and  
> other computer communication should be considered private documents and  
> should not be viewable by law enforcement agencies. It should be treated  
> in  
> the same manner as regular postal mail. If a person is known to be  
> committing a crime via the internet, the ISP can monitor THAT INDIVIDUAL  
> PERSON if given a warrant by the courts but I believe it is  
> unconstitutional  
> to monitor everyone.  
> Sincerely,  
> [REDACTED]  
> [REDACTED]  
> vancouver, BC  
>  
> From Computing Canada, Volume 28, Issue 18, September 13, 2002  
>  
> Canadian Internet service providers face the possibility of massive  
> infrastructure upgrades under a government proposal that would require  
> them  
> to store customer data and disclose it to police and intelligence  
> agencies.  
>  
> According to a 21-page discussion paper posted on the Department of  
> Justice  
> Canada's Web site, the government may try to introduce a law next year  
> that  
> requires ISPs to keep all traffic logs for six months, while allowing  
> authorities to more closely monitor the electronic footsteps of  
> suspected  
> criminals. It also raises the notion of a national database of every  
> Canadian with an Internet account. The government will take comments on  
> the  
> proposal until Nov. 15 at  
> laal@justice.gc.ca.  
>  
>  
>

**Cloutier, Marie**

---

**From:** [REDACTED]  
**Sent:** 2002 Sep 25 4:37 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Justice Dept of Canada Law Proposal

s.19(1)

Dear Sir/Madam,

I am writing to the Justice Department of Canada because I strongly oppose the law proposal to store customer data and to disclose it to police and intelligence agencies.

I oppose this as a private individual and as a Internet business owner.

Yours truly,

[REDACTED]  
Vancouver, CA

**Cloutier, Marie**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Sep 26 3:58 AM  
**To:** la-al@justice.gc.ca  
**Subject:** lawful access

Yet another intrusion into the privacy of law abiding citizen by the government. Not only that but you then will make the ISP's shoulder the cost of the software and upgrades to do your spying. Lets not mince words here this is for the capability of spying on citizens of Canada pure and simple. If this or a like bill is passed it will be yet another nail in the coffin of the freedoms of the people of Canada

[REDACTED]

2002-11-06

000065

From: [REDACTED] s.19(1)  
Sent: 2002 Sep 26 12:47 PM  
To: la-al@justice.gc.ca  
Cc: [REDACTED]  
Subject: Proposed ISP Surveillance Law

Generally speaking, I believe that everyone is supportive of any reasonable law that improves safety and security. The key word here is reasonable, and its definition is in the eye of the beholder! My personal view is that I do not object to any loss of privacy which improves my safety and security, provided that there are sufficient safeguards to protect my privacy such that my safety and security are not at risk. Sorry if this sounds circular and convoluted, but my point is this:

Thanks to CC for the opportunity to express my point of view.

Halifax, Nova Scotia,





**PUBLIC INTEREST ADVOCACY CENTRE**

**LE CENTRE POUR LA DEFENSE DE L'INTERET PUBLIC**

**ONE Nicholas Street, Suite 1204, Ottawa, Ontario, Canada K1N 7B7**

Tel: (613) 562-4002. Fax: (613) 562-0007. e-mail: [piac@piac.ca](mailto:piac@piac.ca). <http://www.piac.ca>

s.19(1)

Senior Counsel

September 27, 2002

Mr. Paul Pierlot  
Senior Advisor  
Lawful Access and Internet Content Policy  
Criminal Law Policy Section, Department of Justice  
East Memorial Building, Room 5024  
284 Wellington Street  
Ottawa, Ontario M4W 1G9

Dear Mr. Pierlot:

**Re: "Lawful Access" Consultations**

The Public Interest Advocacy Centre is a national non-profit organization devoted to the representation of consumer interests in matters involving public utilities, essential services, and public interest issues of broad application to Canadians. PIAC has developed a strong record of consumer advocacy since its inception in 1976, and is widely recognized as an important and influential voice for ordinary consumers in a variety of marketplace issues. PIAC is governed by a distinguished volunteer Board of Directors from across the country, and is supported by member groups and donors representing hundreds of thousands of Canadians. We work closely with a number of other consumer, privacy, and civil rights organizations across the country on issues of national concern.

PIAC is aware of the government's Lawful Access Consultation document, released August 25, 2002, but has had limited time or resources to review the document, or to consult with members, colleagues and other stakeholders on the issues it raises.

We are extremely concerned about the implications that this law reform initiative would have for ordinary Canadians' right to privacy. We need time to consider in more depth the implications of the proposals aimed at facilitating access by law enforcement agencies to information about consumers and users of communications services.

Given the scope of the consultation paper and its potentially significant implications for our members and constituents, we are concerned that it will be very difficult to provide a meaningful response by November 15th.

To ensure that public interest groups are able to provide the government with an informed and comprehensive response to the proposal, PIAC hereby requests that the deadline for written comments be extended to January 31, 2003.

Yours truly,

A rectangular area of the document has been redacted with a grey box, obscuring the signature of the Senior Counsel.

s.19(1)

Senior Counsel

cc. Michael Binder, Industry Canada

Cloutier, Marie

From: [REDACTED] s.19(1)  
Sent: 2002 Oct 02 9:29 AM  
To: la-al@justice.gc.ca  
Subject: Ide sur l'article "Surveillance may force ISP upgrades"

Bonjour,

Je suis étudiant de 3e année à l'Université et j'aimerais bien vous faire part de mon opinion. Suite à la lecture de cet article dans le Communications & Networking j'ai aussi tout de suite pensé à la charte des droits et liberté ainsi qu'au droit à la vie privé. La lutte féroce des fournisseurs internet n'est pas sans doute coûteuse pour celles-ci. L'obligation de faire la mise à jour de leur système et par le fait même d'engager un peu de personnel de plus aura une influence sur le prix final du consommateur. Je suis de l'avis de [REDACTED] sur le fait que la police devrait être celle qui s'occupe de ce dossier. J'ajoute que cette mesure devrait être fait comme celle de l'écoute électronique où il faut un certains nombre de raison afin d'obtenir un mandat pour effectuer les recherches. Il n'est pas mentionné dans l'article par contre quel genre de criminel vous voulez "écouter". Pour ma part suite à l'histoire du présumé enlèvement d'Emili Deblois-Dubé à Varenne, et avant la lecture de cet article, j'ai eu l'idée d'instorer chez moi un ordinateur dédié à prendre un log de tout ce qui se dit dans les "chats" public afin d'augmenter les chances de retrouver avec qui la personne disparue à communiqué avant sa disparition. Je suis sûr qu'il serait possible pour la police de minimalement faire cette intervention et de même obtenir l'autorisation d'écouter les conversations privés. Cette mesure pourrait aussi être utilisé pour les criminels étant basé sur le chat. Pour le reste des activités je vois mal comment les criminels pourraient utilisé internet si ce n'est que des sites de criminel où encore là une association avec les fournisseurs internet pourrait permettre de les écouter au besoin.

J'espère que vous avez apprécié mes commentaires et je vous prie d'agréer mes sentiments les plus distingués.

[REDACTED]  
Technicien en informatique

---

Tired of all the SPAM in your inbox? Switch to LYCOS MAIL PLUS  
<http://www.mail.lycos.com/brandPage.shtml?pageld=plus>



INFORMATION TECHNOLOGY  
ASSOCIATION OF CANADA



ASSOCIATION CANADIENNE DE LA  
TECHNOLOGIE DE L'INFORMATION

OCT 3 2002

October 3, 2002

Richard G. Mosley  
Assistant Deputy Minister  
Criminal Law Policy and Community Justice Branch  
Department of Justice  
284 Wellington Street  
Ottawa, Ontario K1A 0H8

Dear Mr Mosley:

re: **Lawful access consultation**

The Information Technology Association of Canada takes a strong interest in the issues discussed in Justice Canada's *Lawful Access – Consultation Document* (August 25, 2002). In fact, we had a briefing from Justice Canada staff on August 27, and will host a second session next week.

While ITAC has been working towards the current November 15 deadline for comments, we are aware that a number of parties, including several important industry associations, have formally requested that the deadline for written comments on the consultation paper be extended to January 31, 2003.

Given the complexity of the issues involved, and the time required for individuals, companies and associations to develop thoughtful and constructive responses, ITAC would support the granting of such an extension.

Sincerely,



s.19(1)

President & CEO

cc: Michael Binder, Industry Canada

*Paul*  
*L. Rogers*  
*for discussion*  
*Also Nani.*  
*we covered*  
*Clayton's sup*  
*et. à Allan*  
*Nehlling*  
*et Anne*  
*LeBlanc (for sup)*  
*Nani*  
*in*

Cloutier, Marie

s.19(1)

From: [REDACTED]  
Sent: 2002 Oct 07 5:57 PM  
To: 'la-al@justice.gc.ca'  
Subject: Comments on Lawful Access Consultation Document

Hello,

I read the Lawful Access Consultation Document dated August 25, 2002 and do have some comments.

The provision with regards to Virus Dissemination may cause Canada significant harm. Valid research in conducted on viral and other malicious code. Some valid reasons for the possession and sale of these devices could be:

- to identify malicious action(s) performed by the device.
- to test and validate defensive measures that render the device ineffective.

By outlawing the possession of these devices, our domestic information security professionals will be disadvantaged and may not be able to effectively protect critical national infrastructure from hostile attack.

The same Internet resources are currently used by information security professionals and 'crackers' to acquire malicious code (devices). These internet resources may have to change the way in which they operate which may necessitate the sale of these devices to information security professionals in order to continue operations.

In the event that a device is transmitted to a computer (the computer owner is now in possession of the device) without the owners consent, can the computer owner be held responsible for an infraction under this law?

How can the computer owner destroy the device and by so doing return to a situation where he/she is in compliance with the law?

How can consent to acquire a device be ascertained? Downloading a file from the internet does not imply that the computer use knew exactly what the file is or does. If the device is transmitted by email, simply reading your email may become a criminal act.

When one entity uses a computer, another entity manages the computer, and yet a third entity owns the computer, who is in 'possession' of a device that is stored on the computer?

If a device is installed on a computer with out the owners knowledge, is the owner of this computer committing a crime?

This is an expression of my personal opinions and may or may not reflect the opinions of my employer.



UNIVERSITY OF ALBERTA

Date: 2002 October 7

To: Lawful Access Consultation,  
Criminal Law Policy Section  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, Ontario, Canada K1A 0H8  
(via Email: la-al@justice.gc.ca)

s.19(1)

From: [REDACTED]  
Manager, Computing & Network Services  
University of Alberta, Edmonton, Alberta Canada T6G 2H1  
[REDACTED]  
(780) 492-9340

cc: [REDACTED]  
Information Management, Access and Privacy  
Alberta Government Services  
(via Email: [REDACTED])

**With respect to the Department of Justice/Industry Canada/Solicitor General Canada "Lawful Access – Consultation Document", I would like to offer a few comments.**

Firstly, I believe that the essence of the proposal is as follows:

More documented measures need to be put into law to allow enforcement agencies legitimate and ready access to digital records that can assist in investigations to protect the integrity, availability and confidentiality of computer systems and telecommunications networks, and other criminal activities that are aided by communications technology. *[my interpretation of your intent]*

I fundamentally agree with this intent, and appreciate the opportunity to address your discussion document.

My concerns are primarily focused on the burden of enforcement that is being expected of the "internet service provider". In all cases, it is indeed warranted that a service provider be able to comply with a minimal level of technical assistance to an investigative body. However, the expectation that each service provider be appropriately equipped with resources able to handle a non-specific (unidentified) suite of statistical/interception/log information is entirely too open-ended, and (quite likely) too costly for compliance.

A minimum expectation of security readiness needs to be outlined to the service providers. To keep it short, I would consider it reasonable to:

- 1) protect the anonymity of each user of my network, but when directed, be able to reasonably determine and disclose who is using a network "node" within my service (to comply with a lawful investigation)
- 2) disclose and cooperate with investigative agencies on methods to attach interception, seizure and logging equipment to my service.

With your indulgence, I offer you the following points, specific to each section of your document...

The "Service Provider" definition is too generic. By its current definition, a private home individual who operates a home network of more than one machine is a Service Provider. The scope/magnitude of a service provider needs to be refined.

The "European Convention" ratified by the G8 states: "help [...] fight crimes committed against the integrity, availability and confidentiality of computer systems and telecommunications networks [...]" --- this is a very good mission statement, but neglects the "proactive" component; "committed against" does not completely address the anticipation that an offense will occur. I believe that the mission statement should be:

**To establish laws that protect the integrity, availability and confidentiality of computer systems and telecommunications networks.**

*The Consultation Process* -- Proposal point 2) "the need for all telecommunications service providers to ensure that the technical capability in their facilities permits lawful access by law enforcement and national security agencies"

"Technical capability" should not be confused with practicality, or resource readiness. It is not reasonable for service providers to be expected to provide a limitless repository of transactions or data for an undisclosed, potentially limitless duration. It is, however, very reasonable to expect that a service provider be responsible and technically capable of describing appropriate technical methods that may be applied to their environments to comply with specific search/seizure/interception requests by security agencies.

Because of the potentially random, unpredictable circumstances related to a specific investigation, the cost and tools associated with a police seizure or interception should be born by the enforcement agency -- not the service provider.

#### *Requirement to Ensure Intercept Capability*

This area asserts that ISPs currently don't have means to allow enforcement to attach interception equipment. This is false - virtually all network traffic can be intercepted (with the right -- sometimes expensive -- equipment). Keystrokes on a private desktop, however, would be much harder to trap, but I submit that the definition of "interception"

should be refined to establish that a "delivery" of some type, from one device to another, is what needs to be intercepted.

Technically, point-to-point, infrared transmission might be the hardest to intercept – it might be more correct to direct efforts to traditional "network"-based communication, including wireless. Further, "point to point" transmissions (example: between a PDA and a personal computer) do not have a "service provider" by this article's definition)

"A compliance mechanism", for a majority of interceptions, would mean a "packet sniffer" in most cases. It is unreasonable for every service provider to have one of these – it is redundant. If a security agency wants to "sniff", then they should bring the hardware, just as they currently bring 'wire-tapping' gear. It is unreasonable for a business to be compelled to have their own wire-tapping equipment for their numerous network/phone lines. It is very reasonable to have a disclosure document on how network traffic flows, so that security agencies' interception/tapping equipment can be deployed appropriately.

#### *Forbearance*

To specifically identify services providers who are exempt from this compliance is completely unnecessary --- the procedural laws governing lawful search and intercept should account for this. That is, enforcement still needs permission (judicial warrants) to search/intercept; it is at the judicial/warrant request stage that exemptions will be made.

#### *Production Orders*

The concept of having an enforcement agency direct an ISP to produce/deliver arbitrary information, without a judicial warrant, and without regard to the details of the data, is unrealistic. General disclosure of items, such as user lists, would be reasonable. Disclosure of traffic patterns, etc., is often tied to a specific investigation, and would not easily be anticipated beforehand, nor would logs files associated be readily available, gathered or stored. What is the time period for retention? Historical traffic data could be too massive, or specific information not collected. Furthermore, just as in "interception", the resources and capacities (disk space, sniffers, etc) may not be readily available.

#### *Virus Dissemination*

The subject of criminalizing "virus" software should be revised to include all types of "malicious software" – software (or "devices") developed or possessed with the *intent to infringe* on the integrity, availability and confidentiality of computer systems and telecommunications networks.

#### *Interception of EMail*

This section discusses the semantic difference between an "interception", and a "seizure". I believe that this is irrelevant, or at least, should not be tied to directly to Email – data, of any type, can either be intercepted during transit, or seized once it resides at a temporary, or end-destination. Email should not be "singled out".



If the intent of this section is to be able to view communications, care should be given to ensure that newer methods of communication are handled, such as "real-time chat/messaging services". By tying a ruling to specifically handle Email, there is a risk of other communication/transmission techniques being neglected.

*Other mechanisms to provide subscriber and service provider information*

The Internet "standard" or "convention" is to reliably determine what individual is responsible for each Internet address on the network for security purposes. This requirement detracts from a user's right to privacy/anonymity on the Internet. Any law crafted to ensure that an individual can be traced for security purposes, will have to have international acceptance – there are digital safe-havens for anonymity, and only an international law would allow reasonable enforcement of security forensics and policing of illicit activity.

The issue raised relating to who should be the custodian/collector/keeper of identifying data implies that a single entity be responsible for the list of all internet users – this is not feasible. However, it is very reasonable to expect that each service provider be able to determine and disclose any of its individual subscribers.

As a general observation, my experience in the computing industry has taught me that policies that are tied directly to digital aspects are often redundant. As your document points out, much of the search/seizure/interception law already exists in Canada – making policies specific to the telecommunication/computer industry may cloud the issue. For example, disclosure of a patient list in an emergency ward of a hospital is no different than the disclosure of a client list of an internet service provider. Why should there be a different policy/law for each?

In conclusion, I would like to (again) applaud your effort to address digital security and lawful access, and I look forward to reviewing a future document addressing this issue.

I would be more than happy to participate in any discussion that you may have related to this area, should you require any additional resource or input.

Thank you,

[Redacted]  
University of Alberta

[Redacted]  
(780) 492-9340

s.19(1)

**Cloutier, Marie**

**From:** [REDACTED]  
**Sent:** 2002 Oct 07 5:56 PM  
**To:** la-al@justice.gc.ca  
**Cc:** [REDACTED]  
**Subject:** Federal Government Consultation Paper -- Lawful Access Consultation Document --  
University of Alberta comments



LawfulAccessUofA.pdf

Good afternoon.

I would like to offer the following comments, related to the Government of Canada "Lawful Access - Consultation Document", based on a PDF forwarded to me from my colleague at the Alberta Government IT division.

The 21-page document was dated August 25th, 2002, and solicits comments via email to this email address.

I respectfully submit these comments, in my capacity as a manager of IT services for the University of Alberta -- we operate a fairly large "ISP" (by your definition) - 60,000 computing IDS, and I believe decisions made in the area of disclosure, search, seizure, and interception will certainly affect my University's operating strategies and budgets.

Should it not be too late, I would like to offer to participate in any discussion groups that you may be organizing to address this issue.

The enclosure is a 4-page PDF file, suitable for viewing by Adobe Acrobat version 5.

Thank you,

[REDACTED]  
s.19(1)

University of Alberta  
Edmonton, Alberta Canada T6G 2H1  
[REDACTED]



s.19(1)

Executive Vice President  
Corporate Affairs & General Counsel

# 2002 - 020963  
OCT 9 2002

8<sup>th</sup> Floor  
555 Robson Street  
Vancouver, British Columbia  
Canada V6B 3K9

604 697-8020 Telephone  
604 437-8560 Facsimile

October 8, 2002

Richard G Mosley QC  
Assistant Deputy Minister  
Criminal Law Policy and Community Justice Branch  
Department of Justice  
284 Wellington Street  
Ottawa, Ontario K1A 0H8

Dear Mr. Mosley

On August 25, 2002, a paper was released by Justice Canada entitled: Lawful Access - Consultation Document soliciting public input on its proposals. In early September, I understand that a number of associations including:

- the Canadian Cable Television Assoc,
  - the Canadian Assoc of Internet Providers
  - the Canadian Wireless Telecom Assoc and
  - the Canadian Advanced Technology Assoc
- wrote jointly to Justice Canada to request an extension of the period allotted for the submission of comments.

Since that time, TELUS staff have had an opportunity to complete an in depth review of the paper and also to attend a meeting hosted by your colleague, Michael Binder, of Industry Canada and to gather insight there from the presentations and answers provided.

It is even more clear now that the privacy, technical, operational and service issues that implementation of the paper's proposals would have on TELUS need a comprehensive, thoughtful response. Given the nature of the work required to carry this out, I too am now more convinced than ever that we will need an extension to the comment period to provide useful, constructive input to these issues.

I would like to reiterate the request made already by CCTA, CAIP, CWTA and CATA to extend the deadline for written comments to January 31, 2003.

Yours truly,



s.19(1)

cc. CCTA,  
CAIP  
CWTA  
CATAAlliance  
Michael Binder, Industry Canada  
Allan MacGillivray, Industry Canada  
Mr. Paul Pierlot

**Cloutier, Marie**

**From:** [REDACTED] s.19(1)

**Sent:** 2002 Oct 10 9:58 AM

**To:** la-al@justice.gc.ca

**Subject:** I teach database theory at the college and university level, and write database systems for  
I teach database theory at the college and university level, and write database systems for healthcare... and I  
have worked with databases for over a quarter century.

I believe the unified national database of every Canadian using the Internet is on the logical level very enticing for security purposes, yet on the practical level, as evidenced by my trips worldwide, including to Chile, Russia, and the Ukraine, and centralization of information leads rapidly to the abuse of power. It seems a human trait and condition that abuse of power will occur. Abuse of security will also occur.

Maintaining the proposed database of this type and "logs" will, in my global informed opinion, cause more harm a nationwide level than good, penalizing the masses of good Canadians and jeopardizing their privacy and security, for a small and imaginary enemy.

With all best wishes, I remain,

Sincerely,



THIS TRANSMISSION IS INTENDED ONLY FOR THE ADDRESSEE, IT MAY CONTAIN PRIVILEGED OR CONFIDENTIAL INFORMATION. ANY UNAUTHORIZED DISCLOSURE IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS TRANSMISSION IN ERROR, PLEASE NOTIFY US IMMEDIATELY SO THAT WE MAY CORRECT OUR TRANSMISSION. PLEASE THEN DESTROY THE ORIGINAL. THANK YOU.



Office of the Information  
and Privacy Commissioner

October 11, 2002

#410, 9925 - 109 Street  
Edmonton, Alberta  
Canada T5K 2J8  
Tel.: (780) 422-6860  
Fax: (780) 422-5682  
Website: [www.oipc.ab.ca](http://www.oipc.ab.ca)  
Internet: [ipc@planet.eon.net](mailto:ipc@planet.eon.net)

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, Ontario  
K1A 0H8

**Attention: Justice Minister Martin Cauchon**

Dear Minister Cauchon:

**Re: Lawful Access Consultation**

The Department of Justice, with the Portfolio of the Solicitor General of Canada and Industry Canada, has invited comments on proposals to amend the *Criminal Code* and other federal Acts that regulate access to telecommunications for law enforcement purposes. These proposals are designed partly to allow Canada to ratify the European Convention on Cybercrime (the "Convention").

I agree in principle that law enforcement organizations must get effective access capabilities to new communication technologies, for both domestic and international law enforcement. Canadian-based internet service providers (ISPs) should be required to have the technical capability to afford lawful intercept capability to an internet-based communication.

I have these comments on privacy for your consideration.

**Buried Privacy Issues**

The proposals in the consultation paper are like loose threads, that, if tugged on, unravel and reveal many underlying questions about privacy that are buried in the larger issues. For instance: should it be lawful to open an e-mail account in Canada without a client providing basic customer information for each e-mail address? What are the appropriate kinds of personal information that could be collected by Canadian ISPs? What degree of anonymity on-line would be permissible under the proposed amendments? Would anonymous re-mailing of e-mail within Canada remain lawful? Would encrypted e-mail be permitted within Canadian borders, and if so, on what terms?

I encourage you to make sure that these basic and critical questions are put to Canadians directly within the consultation process.

## **General vs. Specific Measures**

The Convention states that the parties to it must ensure that they implement the Convention in a manner that respects domestic human rights and liberties.

The consultation paper presents both general and specific measures to create lawful access to internet communications. Interceptions and seizures of internet communications, both content and traffic data, should be as narrow and specific as possible. Routine and exploratory electronic surveillance on a large scale must not be allowed. Overbroad measures would impair privacy rights and run afoul of section 1 of the *Charter of Rights and Freedoms*.

**Treat internet e-mail as a communication in which senders and receivers have a reasonable expectation of privacy under the *Canadian Charter of Rights and Freedoms***

The consultation paper raises the key issue of whether an e-mail should be considered a private communication under the *Criminal Code*. In 1993, the Supreme Court of Canada in *R. v. Plant* unanimously held:

...section 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choice of the individual [at para 20]

An e-mail, which can contain text, sound and graphics files, is a rich source of intimate personal information about the sender, and, potentially, the recipient. The Alberta courts have affirmed that the recipient of the content of an internet e-mail enjoys a Charter-based reasonable expectation of privacy in that communication: *R. v. Weir*, [1998] A.J. No. 155, affirmed [2001] A.J. No. 869 (Ab.C.A.). In *Weir*, the header of an e-mail was likened to address information on the outside of a mailed envelope, and was held to carry a lower expectation of privacy than the information inside. In *R. v. Weir*, the issue of how much lower the expectation of privacy is in an e-mail header was left unanswered.

## **Data Retention and Preservation**

Many people have multiple e-mail accounts, both at home and at work. It is not uncommon for people to terminate e-mail accounts and create new ones with new ISPs that offer a better deal. Having considered the logistics of a creating and maintaining a comprehensive national database of current e-mail customer account information, I think it is an unworkable idea that would drain resources better used elsewhere.

I urge you not to draft provisions that would require ISPs to retain all traffic data and content for a specific period solely the purposes of a hypothetical law enforcement action. Such measures would be overbroad and could seriously harm Canadian privacy, and the business of Canadian-based ISPs. Canadians could flee to ISPs based outside of Canada

to preserve their privacy, and seriously damage the industry that underpins domestic electronic commerce.

Yours truly,

s.19(1)

Frank J. Work, Q.C.  
Information and Privacy Commissioner





# Toronto Police Service

40 College Street, Toronto, Ontario, Canada. M5G 2J3  
(416) 808-2222 FAX (416) 808-8202  
Website: www.TorontoPolice.on.ca



s.19(1)

Chief of Police

DOJ 021236  
MCUEA2

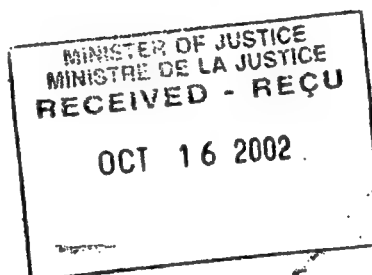
File Number: .....

150017

October 15, 2002

The Honourable Martin Cauchon  
Minister of Justice  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

Via Facsimile: (613)990-7255



Dear Mr. Cauchon,

I have been informed that representatives of the telecommunications industry and/or organizations representing the industry have requested an extension for submission of comment to the lawful access consultation document from November 15<sup>th</sup>, 2002 until January 31<sup>st</sup>, 2003. As Chair of the Lawfully Authorized Electronic Surveillance (LAES) representing the interests of law enforcement in these issues, I must protest any delay in the process. The LAES has been involved and in fact introduced this initiative over five years ago. The Law Amendments Committee (LAC) of the C.A.C.P. in turn presented these concerns to the D.O.J. in November of 1999. We appreciate that the exercise is time consuming due to its complex and comprehensive nature and your staff is expending great effort to move the process in timely fashion.

The telecommunications industry has been consulted over the last five years in this regard. There has been liaison, both official and otherwise, with the LAES and other levels law enforcement during this period.

- The LAES has formally participated in the meetings of the Network Security Working Group of the CRTC Interconnect Steering Committee, an industry group formed to address the impact of deregulation. All issues concerning lawful access were discussed at these meetings.
- Law enforcement has participated in an Industry Canada consultation process dealing with the issues of encryption and Internet security. The needs of law enforcement regarding lawful access were addressed in this process.
- Law enforcement and the LAES have participated in the Telus tariff application before the CRTC known as 99/04 and the subsequent public notices known as 99/10 and 99/17. Many of the same issues were addressed in these processes.
- Law enforcement and the LAES have participated in the Bell Canada show cause process known as 6178 concerning a CNA tariff. Once again, some of these issues were addressed in this ongoing process.

*To Serve and Protect - Working with the Community*

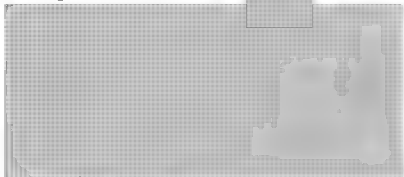
000083

All of these procedures have been public. All of the responses are public documents. The position of law enforcement has been restated consistently throughout.

Over the past five years, law enforcement and the LAES have liaised with all large industry entities. In fact, operational units of law enforcement and national security work with the industry, both large and small, on a daily basis. They know us and are familiar with our requirements. They know too that law enforcement has been seeking to maintain lawful access ability through legislation. Your consultation document has been expected and they should be sufficiently prepared to respond appropriately within the prescribed time frame.

Delaying the procedure is not in the public interest. Presently, law enforcement and national security are conducting investigations that are being compromised due to lack of ability on certain technologies and lack of legal process to support these investigations. There are public safety implications the longer this situation remains in effect.

Respectfully Yours,




s.19(1)

Chair - LAES

Cc The Honourable Lawrence MacAulay  
Solicitor General of Canada  
Via facsimile: (613)995-2754

The Honourable Allan Rock  
Minister - Industry Canada  
Via facsimile: (613)992-0302



Chair - Law Amendments Committee  
Via facsimile: (613)236-7536

**Cloutier, Marie**

---

**From:** [REDACTED] s.19(1)

**Sent:** 2002 Oct 15 3:12 PM

**To:** la-al@justice.gc.ca

**Subject:** Re: Will Canada's ISPs become

Why would they do that isn't our childrens education or our health more important than spying on us, its like thats a lot of money to spend I dont think that they should implement this law until they upgrade our hospitals or schools. All they think of is spending money on stupid things.

2002-11-06

000085

**Cloutier, Marie**

---

**From:** [REDACTED]  
**Sent:** 2002 Oct 16 4:12 PM  
**To:** 'la-al@justice.gc.ca'  
**Subject:** Lawful Access Consultation

Hi there,

My comments relate to the statement in the conclusion of the document where it is indicated that Government of Canada Officials expect to meet with various parties this fall to discuss the Lawful Access paper.

Alberta Innovation and Science representatives are interested in meeting with representatives from the Departments of Justice and/or Industry Canada to further discuss issues arising from the Consultation Paper.

I would appreciate it if you could provide me with the appropriate contact information.

Thank you,

[REDACTED]  
Innovation and Science s.19(1)  
Government of Alberta  
[REDACTED]

This communication is intended for the use of the recipient to which it is addressed, and may contain confidential, personal and or privileged information. Please contact us immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. Any communication received in error, or subsequent reply, should be deleted or destroyed.



October 18, 2002

Richard G. Mosley QC  
Assistant Deputy Minister  
Criminal Law Policy  
and Community Justice Branch  
Department of Justice  
284 Wellington Street  
Ottawa, ON K1A 0H8

333 Bloor Street East  
Toronto, Ontario M4W 1G9  
Tel. (416) 935-7211  
Fax (416) 935-7719  
rci.rogers.com

s.19(1)  
Vice-President  
Government & Inter-carrier Relations

Dear Mr. Mosley:

I am writing to you today to express the full support of Rogers Wireless Inc. ("RWI") for the jointly submitted request of a number of industry associations that the Department of Justice ("the Department") extend the comment period associated with the consultation paper released by the Department on August 25, 2002 entitled: Lawful Access – Consultation Document.

Specifically, the following industry associations have requested that the comment period be extended to January 31, 2003:

- the Canadian Association of Internet Providers
- the Canadian Cable Television Association
- the Canadian Wireless Telecommunications Association

RWI strongly agrees with these associations, and the numerous stakeholders they represent, that the complexity and scope of the issues under consideration in the Consultation Document warrant the provision of an extended comment period.

The requested extension would permit all parties, including RWI, to prepare and submit more comprehensive and constructive comments to the Department than will be possible within the existing comment period.

**Thank you in advance for your consideration of this request.**

Sincerely,

**s.19(1)**

Cc: CAIP  
CCTA  
CWTA  
Michael Binder, Industry Canada  
Allan MacGillivray, Industry Canada  
Paul Pierlot, Department of Justice



Rogers Wireless Inc.  
333 Bloor Street East  
Toronto, ON M4W 1G9

FAX COVER FORM:

s.19(1)

Tel. No. 416-935-7212  
Fax No: 416-935-7719

From: ☒ [REDACTED] Vice President, Government & Inter-carrier Relations  
☐ [REDACTED] - Executive Assistant  
☐ [REDACTED] - Administrative Assistant  
☐ [REDACTED] - Director, Government Relations  
☐ [REDACTED] - Director, Inter-carrier Relations

To:

Name: Mr. Michael Binder / Mr. Allan MacGillivray / Mr. Paul Pierlot  
Fax #: (613) 952-1203 / (613) 941-1399 / 613-941-9310  
Location: Industry Canada / Industry Canada / Dept. Of Justice

Date: October 18, 2002

Time: \_\_\_\_\_

No. of Pages (including Cover): 3

Remarks:

If you have any trouble with this transmission please call the sender at the number above.

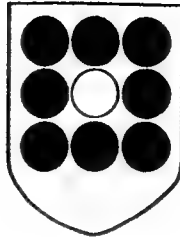
The information contained in this telecopy is intended only for the use of the recipient named above. This telecopy may contain privileged, confidential or undisclosed information. If the reader of this telecopy is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this telecopy in error, and that any review, dissemination, distribution or copying of it is strictly prohibited. If you have received this in error, please notify us immediately by telephone (if necessary call the number above collect) and return the original transmittal by mail. Thank you.

© Rogers Wireless Inc.

000089

CANADIAN  
CIVIL LIBERTIES  
ASSOCIATION

394 Bloor Street West, Suite 200  
Toronto, ON M5S 1X4  
Telephone (416) 363-0321  
FAX (416) 861-1291  
E-mail ccla@ilap.com



ASSOCIATION  
CANADIENNE DES  
LIBERTES CIVILES

394 rue Bloor Ouest, Suite 200  
Toronto, ON M5S 1X4  
Téléphone (416) 363-0321  
Télécopieur (416) 861-1291  
Courriel ccla@ilap.com

s.19(1)

October 22, 2002

Lawful Access Consultation  
Criminal Law Policy Section  
Department of Justice  
5<sup>th</sup> Floor - 284 Wellington Street  
Ottawa, Ontario  
K1A 0H8

To Whom It May Concern:

Re: Lawful Access - Consultation Paper

Despite our inability to attend the consultation meeting, we thought it might be useful to convey some of our responses in writing.

In the opinion of the Canadian Civil Liberties Association, any consideration of increasing the power of the state to eavesdrop on citizens requires from the government a clear demonstration of the need. In view of the considerable powers already available in this regard, the mere invocation of 9-11 will not suffice. The public needs to know precisely *why* the current powers are not enough.



The reason for this is the important place that personal privacy occupies in the value structure of the Canadian people. When personal information about any of us passes from our control, our sense of dignity and self-respect undergo significant erosion. And, to whatever extent such personal information reveals our political plans and predilections, we suffer a commensurate diminution of our free speech, freedom of assembly, freedom of association, and right to dissent.

The application of these considerations is particularly appropriate to the Internet. The right to explore and communicate in anonymity has transformed the Internet into a special sanctuary for its users. By itself, the mere prospect of governmental invasion is likely to create a chill over Internet activity; the actual invasions are likely to exacerbate the chill.

For all of these reasons, the Canadian Civil Liberties Association takes the position that any invasion of these electronic sanctuaries should require the most compelling circumstances and exacting safeguards. Thus far, the government has not made the case.

In any event, there would be no excuse to adopt a *lower standard* that would allow the police to monitor Internet traffic, including the origin, direction, time, duration, destination, and termination of any transmission. The power to perpetrate such an encroachment is capable of revealing a vast amount of medical, sexual, political, social, and psychological information concerning the Internet users. Thus, there should be no question of adopting a lower standard for such eavesdropping.

CCLA objects also to the scope of the proposed power to intrude on those who are found on targeted premises. The mere coincidence of being lawfully present on suspected premises is not a sufficient basis to require anyone found on such premises to provide any items or materials that may be on their persons. No less unacceptable is the idea that, by itself, the mere presence of people on such premises could justify imposing any kind of personal search on them. Apart possibly from those who are reasonably believed to be concealing the contraband at issue, there should be no such power to invade the persons of any individuals.

To whatever extent such additional powers are contemplated, the enabling statute should contain provisions designed to ensure the reliability and security of the information involved. An additional safeguard that would have to accompany any such provision is a requirement for the minimization of any interception. Since some of the technology will now make it possible to seek material by using such devices as simple key word searches, the enabling legislation should follow suit. The judges who grant warrants should be explicitly required to narrow their authorizations so that, as much as possible, unnecessary invasions of privacy can be avoided.

Sincerely



s.19(1)

General Counsel

Cloutier, Marie

From: [REDACTED] s.19(1)  
Sent: 2002 Oct 23 4:45 PM  
To: la-al@justice.gc.ca  
Cc: [REDACTED]  
Subject: Email privacy and the Lawful Acciss

I have a question regarding interception of email. It stems from an email disaster I encountered when my ISP seized and withheld my email in order to leverage payment from me. Briefly, here's what happened:

Without prior notice my ISP, Inter.net Canada Ltd., changed my password so I couldn't log on to their server. I contacted them and was told I owed them \$106.87. I disputed this vigorously and, when it became clear the dispute couldn't be resolved, I decided to give up the email address I'd had for 7 years and dumped this ISP, signing up with another provider that same day.

What this company didn't tell me was they had kept my email address open, and continued to absorb all my email for weeks after they initially suspended my account. When I figured it out what was going on weeks later I called and asked them to forward my email and shut down the address. I was bluntly told "not until you pay us the \$106.87 you owe us".

After chewing my way up the food chain into the US parent company I eventually got this email back without paying this money. Unfortunately, one of the seized emails was from an Executive Producer at the Discovery Channel contacting me regarding a job opening on her show. This was potentially a \$65,000 contract.

I subsequently discovered that all ISP's in Canada have this practice as standard operating policy: accounts that are viewed by them to be in arrears are 'suspended', but the email account is held open and continues to absorb email without the sender knowing the recipient has no access to the message, and without the recipient knowing there are messages for them. Since I've been going after them on this issue, Sympatico has stated it has discontinued this practice.

I filed a complaint with the federal Privacy Commissioner and he recently issued a finding in my favour. But he only requires that ISP's make it clear in their Terms & Conditions that 'suspension' means you'll be locked out of your active email account. He 'recommends' that they should all stop doing it altogether since, as I vigorously pointed out to them, no sender agrees to any ISP's Terms & Conditions.

The other email seized from me for four weeks was from a contractor who I had emailed asking if he was available to do some work on my house. He also lost that business opportunity because his reply was withheld from me.

As a result of the Privacy Commissioner's finding I have filed in Federal Court under the Personal Information and Electronic Documents Act (PIPEDA).

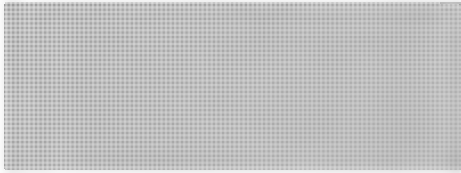
Can you advise me of how the law views this practice in light of Part XV of the *Criminal Code* and under s. 15 or 16 of the *Competition Act*?

Can you also advise me of how this is addressed in your current Lawful Access Consultation

Process?

Thank you in advance for looking into this matter. Please contact me if you have any questions.

Sincerely,



s.19(1)

## **Saskatoon Police Service**

*"In Partnership With The Community"*



October 24, 2002

Department of Justice Canada  
Criminal Law Policy Section  
284 Wellington Street, 5<sup>th</sup> Floor  
Ottawa, Ontario  
K1A 0H8

Dear Sir/Madam:

**Re: Lawful Access Consultation**

This letter is in response to correspondence received requesting feedback on the Lawful Access Consultation Document.

The comments included below, are in response to the issues identified on Page 19 of that report.

The Charter of Rights and Freedoms and the Criminal Code more than adequately protect Canadians against invasion of their privacy. Keeping those two pieces of legislation in mind, there would be nothing wrong with establishing a database of CNA and LSPID information, administered by the Royal Canadian Mounted Police, in much the same way as C. P. I. C. is.

Wherever possible an Internet Service Provider should be aware of all who access their services. Legislation should be in place to collect and retain such information with a view to uploading it to the database.

Mechanisms should be created or adapted to provide LSPID for Internet Service Providers. This would be an important investigative tool for law enforcement, much in the same way it applies to telephone subscriber information. Generally speaking this information is not the cornerstone of any investigation, but a helpful building block which, when added to other evidence from a variety of sources, makes for a compelling body of evidence.

As far as who should pay, I would suggest that the federal government might consider cost sharing with the Internet Service Providers, the cost of providing the interconnectivity required to facilitate a national database. Both the providers and those who access the database would benefit from it in that any I. S. P., who is carrying on business for a lawful purpose, would not want their subscribers using their service for criminal purposes. The federal government would benefit in being able to assist law enforcement and national security interests, by providing the valuable information contained within the database.

● Page 2

October 24, 2002

Whereas any of the above actions could be looked upon as "Big Brother" tactics, we cannot abrogate the task of policing cyberspace. The public looks to the police for protection, and we must have the tools to accomplish that purpose.

I trust these comments will assist you in developing the legislation required.

Yours truly,

s.19(1)

Superintendent  
Criminal Investigations Division

KR/dr

Cloutier, Marie

From: [REDACTED] s.19(1)

Sent: 2002 Oct 25 10:05 AM

To: [REDACTED]

Cc: [REDACTED] la-al@justice.gc.ca

Subject: Re: spying...

1. The biggest thing that sucks with this, is poor mom& pop ISPs will be forced to install expensive equipment, so that government agencies can snoop around peoples' e-mail and data transmissions. No matter who picks up the tab, the costs will eventually be paid by the consumer.
2. As with the "Carnivore" system, created by the FBI\CIA a couple years ago (and allegedly, made illegal), the simple hourly volume of email and data transmissions should negate any fear of the government snooping on "minor offenses". However, by putting words like "bomb" or "jihad" in your email, usually means that some poor FBI nerd may read your transmission. Hi, Mr. FB!guy, I'm one of the good guys =)
3. If terrorists and/or other criminal entities are stupid enough to communicate via data transmissions, they would probably encrypt the transmission using PGP (which is free, BTW), or something similar. We install PGP for our exec's here, where I work... These encryption schemes make it impossible to very difficult for \*anyone\* to intercept. The US government has tried to make public data encryption illegal, or at least put in some "backdoors" in these apps so that they can intercept. However, the US government tends to ignore the fact that the first "W" in "WWW" stands for World ! Past lessons learned (ie porn, spam) shows that the internet is almost impossible to regulate...
4. Once some entity tries to stop or regulate something on the internet, the latest being the evil RIAA trying to stop peer-to-peer networks such as Morpheous, the internet community (and yes, unfortunately, terrorists...) usually finds a way around it. It was recently discovered that terrorists were communicating via simple .jpg (picture) file attachments...
5. The silver lining in all this is (as this will probably pass anyho), hackers and virus writers (a.k.a. script kiddies) world-wide, better think twice before they start screwing around ! These people are now labelled to be terrorists and will be punished as a terrorist would be. The US is becoming very crafty in catching & prosecuting these people... This is a good thing, as this is becoming a real pain in everyone's ass !

my two cents,  
S.

----- Original Message -----

From: [REDACTED]

To: [REDACTED]

Sent: Friday, October 25, 2002 9:03 AM

Subject: spying...

If after reading the following Globe article...

<http://www.globetechnology.com/servlet/GAMArticleHTMLTemplate?>

[tf=globetechnology/TGAM/NewsFullStory.html&cf=globetechnology/tech-config-neutral&slug=TWGEIS&date=20021003](http://globetechnology/TGAM/NewsFullStory.html&cf=globetechnology/tech-config-neutral&slug=TWGEIS&date=20021003)

you decide to send any comments regarding this issue to the government you can visit:

[la-al@justice.gc.ca](mailto:la-al@justice.gc.ca)

The deadline for submissions is Nov. 15, 2002.

If you want to read the proposal by the Department of Justice in full (may be a bit much for some!) you can find it at:

[http://www.canada.justice.gc.ca/en/cons/la\\_al/](http://www.canada.justice.gc.ca/en/cons/la_al/)

ah

---

Get faster connections -- switch to MSN Internet Access! [Click Here](#)



Cloutier, Marie

s.19(1)

From: [REDACTED]  
Sent: 2002 Oct 25 4:41 PM  
To: la-al@justice.gc.ca  
Subject: Feedback on ISP intercept / tracking proposal

As a Canadian citizen I would like to provide my limited feedback on the recommendation of internet intercept and tracking proposals.

Below I mention two specific points which provide contrast to our provided freedoms and rights, first I have an overall opinion in regards to telecommunications tracking.

I consider it a grave danger to allow any special degree of tracking to be established with respect to telecommunications, particularly the internet. My argument is based on drawing a parallel, such that tracking internet activity is akin to tracking the reading habits of an individual who frequents the public library. Any access to this data would be a breach of individual privacy. Additionally, since any information obtained this way would be considered circumstantial in a court of law: that said, as a volume of circumstantial evidence is often weighted comparable to direct evidence, it may become easier for the police authorities to amass such volumes of circumstantial evidence rather than use investigative techniques to obtain direct evidence.

In the heading "Access to Hidden Records" I am concerned on the provision to allow an obstruction charge if hidden information is not revealed. It is not possible to distinguish whether an individual has indeed hidden the information, or simply does not have the requested information. These leaves the possibility to pad search warrants with countless items to ensure an obstruction charge allowing for detainment, furthered questioning, or marking the individual as non-cooperative -- even if said individual is not guilty of any suspected crimes.

Under "Other mechanisms to provide subscriber and service provider information" there is mention of a potential central registry for maintaining subscriber information. For two reasons I would hope such a central registry is not formed: a) it necessarily disrupts an anonymity that many individuals presently rely on to convey their political and social opinions; and b) such a database, and potential access to this database, allows for abuse in the form of blanket profiling (or preemptive policing) which is an abuse of privacy, civil liberties, and overall of questionable police ethics.

[REDACTED]

I know the truth is a myth, but that doesn't mean I'll stop searching for it.

Cloutier, Marie

s.19(1)

From: [REDACTED]  
Sent: 2002 Oct 27 12:05 PM  
To: la-al@justice.gc.ca  
Cc: [REDACTED]  
Subject: Lawful Access - Consultation



Lawful Access  
Consultation.doc...

Dear Sir or Madam;

Attached is a letter setting out my views with regards to the above.  
Yours truly,

[REDACTED]  
Friends of Simon Wiesenthal Center for Holocaust Studies



*Friends of Simon Wiesenthal Center*  
**FOR HOLOCAUST STUDIES**

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington Street  
Ottawa, Ontario  
K1A 0H8

October 27, 2002

Dear Sir or Madam:

Prior to commencing, it should be absolutely understood that anything stated herein are only the views of the author and that any opinions expressed are **not** to be construed as the views, opinions, position or attitude of the Simon Wiesenthal Center or any of its branches or personnel anywhere in the world.

Friends of Simon Wiesenthal Center for Holocaust Studies (Friends) has had an opportunity to review the "Lawful Access – Consultation Document", dated August 20, 2002.

Friends is an independent entity, which is incorporated in Canada and has over 20,000 Jewish and non-Jewish members. Friends is a human rights organization, which strives to ensure that all Canadians live in dignity and freedom. Friends believes that racism, hatred and intolerance have no place in the Canadian community. For that reason, Friends is a leader in Internet monitoring and the training of police and security officials on how to trace and counter criminal and terror sites on the Internet.

For the past five years, in conjunction with other experts around the world, an annual CD-ROM report entitled "Hate on the Internet" has been produced and distributed to law enforcement officials, security agencies, Governments and educational institutions.

In June 2000, Friends, the Internet industry and the Canadian Government sent delegates to an international conference in Germany that dealt with Hate on the Internet. The Berlin Declaration, which was adopted at the end of the meeting, made it clear that hate (like terrorism, fraud, child pornography and other illegal activities) will continue to prosper as long as the Internet itself remains virtually ungovernable.

8.17  
While freedom of speech, of association and commerce are important values and must be maintained and preserved, the world does not function within such absolute freedoms. Virtually all activity is regulated to varying degrees. This is especially true in the communications and media industries. Whether we write letters, speak on telephones or communicate via ham radio, there are statutes that restrict our absolute uses of these mediums. For the most part, Canadians understand why we need regulations. Without getting into issues of censorship (and for the record, Friends does not advocate censorship), most people accept that Government intervention is required, to varying degrees, in a variety of fields for numerous political, social and economic reasons.

Should the authorities have the right to access and obtain personal information and / or intercept personal communications that originates or travels through the Internet? The short answer is yes.

If one accepts the premise that lawful interceptions are a necessary tool for combating crime, terrorists and preserving national security, then there can be no argument for not extending that lawful access to the Internet. The only caveat is that the authorization for such orders (whether they be production orders, preservation orders or interception orders) must be judicially sanctioned and subject to court challenges in accordance with the *Charter of Rights and Freedoms*.

The only further comment that we would make is that none of the above is possible unless all Internet service providers are obligated to maintain a proper log of registered users. Cyber squatting and identity theft and false identifications are the bane of the Internet. As long as sites can be obtained under aliases and maintained under fictional names with false addresses and fake contacts, chaos will reign and law-abiding individuals and corporations will be victimized and law enforcement authorities will be frustrated in their ability to investigate and prosecute offenders.

In general, therefore, we would support the principle of lawful access to the Internet.

Should you have any questions or if we could be of any further assistance, please don't hesitate to contact the undersigned.

Yours truly,

s.19(1)

Friends of Simon Wiesenthal Center for Holocaust Studies  
416-864-9735 (office)

Cloutier, Marie

---

From: [REDACTED] s.19(1)

Sent: 2002 Oct 28 1:35 PM

To: la-al@justice.gc.ca

Subject: Comments on legislative proposals

To whom it may concern,

I am a Computer Science professional, and after briefly reading an online document suggesting new internet governing legislation\* I have become concerned with it's possible adverse effects on the privacy of Canadians.

The part that I find most disturbing is the idea of a national database of internet users. This could effectively eliminate the ability of Canadians to log on to the internet anonymously.

The ability to remain anonymous is fundamental to free speech. It allows people to express their opinions without fear of reprisal.

I believe that a law with this much power is bound to be misused, and therefor I ask that you please reconsider enacting this or such laws.

Though I am aware that some sacrifice is necessary, I do not believe that most Canadians would agree with completely sacrificing privacy in the name of security.

Thanks you,

[REDACTED]  
\* [http://www.canada.justice.gc.ca/en/cons/la\\_al/e.html#24](http://www.canada.justice.gc.ca/en/cons/la_al/e.html#24)

**Cloutier, Marie**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Oct 28 11:44 AM  
**To:** 'consultations@canada.justice.gc.ca'  
**Cc:** 'la-al@justice.gc.ca'  
**Subject:** FW: Lawful Access consultation

Please see attached. Did not go through the first time. Thank you.

[REDACTED]  
Montreal (Quebec)

-----Original Message-----

**From:** [REDACTED]  
**Sent:** Wednesday, October 23, 2002 10:50 AM  
**To:** 'consultations@canada.justice.gc.ca'  
**Subject:** Lawful Access consultation

I understand comments on the Lawful Access questions are due November 15, 2002. Will the comments be posted on your web site? If so, approximately when? And if not, what is the process to obtain a copy?  
Thank you in advance for your assistance.

[REDACTED]  
Montreal (Quebec)

**Pages 105 to / à 123  
are withheld pursuant to section  
sont retenues en vertu de l'article**

**13(1)(d)**

**of the Access to Information Act  
de la Loi sur l'accès à l'information**

D02-023193  
MCUED3

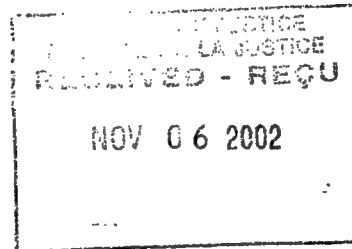
President and Chief Executive Officer  
Président et chef de la direction

s.19(1)

Le 1<sup>er</sup> novembre 2002

270201

L'honorable Martin Cauchon, C. P., député  
Ministre de la Justice  
et procureur général du Canada  
Ministère de la Justice  
284, rue Wellington  
Ottawa (Ontario) K1A 0H8



**Objet : Consultation sur l'accès légal:**

Monsieur le Ministre,

Je vous écris suite à la consultation amorcée par la publication du document conjoint des ministères de la Justice, de l'Industrie et du Solliciteur général sur l'accès légal, le 25 août dernier et ce, au nom de l'Association canadienne des télécommunications sans fil (ACTS).  
Nous croyons que cette consultation sera plus productive si on fournit plus de détails aux intéressés.

Le 15 octobre, les membres de l'ACTS ont eu l'occasion de rencontrer des fonctionnaires des trois ministères susmentionnés. Bien que ces représentants aient aidé à éclaircir divers points du document de consultation, il en reste d'autres, d'importance critique, à propos desquels des questions subsistent.

Tout projet de loi modifiant la législation sur l'accès légal et tout règlement en découlant devrait, à notre avis, faire partie de la consultation publique. Bien qu'il soit vrai que nous aurons sans aucun doute la possibilité de présenter des observations sur un tel projet dans le cadre normal de la procédure parlementaire, il nous semble tout aussi important d'avoir la possibilité de le faire, de manière aussi complète, au sujet de tout projet de réglementation et de norme dont s'assortirait le projet de loi.

Pour contribuer de façon vraiment utile à l'examen de la politique proposée, nos membres doivent saisir toute l'ampleur de ce qu'on attendrait d'eux selon cette proposition. On nous dit que ces exigences seront détaillées dans les nouveaux règlements. Toutefois, aucun projet de règlement ni énoncé des exigences qu'il comportera n'a été mis à notre disposition pour que nos membres et nous puissions l'étudier et présenter des observations.

.../2



2/...

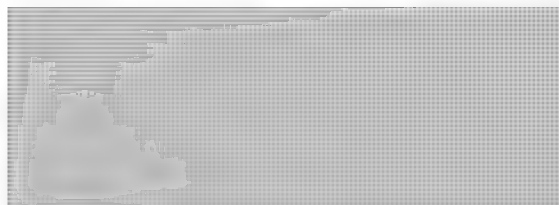
De plus, certains des éléments clés de la proposition ne sont pas définis. Par exemple, il y est dit que tous les fournisseurs de services de télécommunications seraient tenus d'assurer au moins une « capacité de base d'interception ». Il y est dit également que ces fournisseurs devraient supporter le coût de l'accès légal en cas d'« amélioration significative » de leur système ou réseau. Or, ni l'une ni l'autre de ces expressions n'est définie.

Nous reconnaissons que l'accès légal est un outil indispensable pour les responsables de la sécurité nationale et de l'application de la loi. Nous souhaitons présenter des observations constructives concernant la politique et le projet envisagés, mais nous pourrions difficilement le faire à moins qu'on ne nous fournisse le genre de détails susmentionnés.

Nous avons hâte de nous pencher sur ces renseignements afin de pouvoir faire un apport éclairé à cette importante consultation.

Si vos fonctionnaires ou vous-même avez besoin de plus de précisions sur les renseignements qui nous semblent nécessaires, veuillez ne pas hésiter à communiquer avec notre vice-président aux affaires réglementaires et de l'industrie, [REDACTED] que vous pouvez joindre au (613) 233-4888, poste [REDACTED] ou avec moi.

Avec mes remerciements anticipés, je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma très haute considération.



s.19(1)

c.c. : L'honorable Wayne Easter, C. P., député, solliciteur général  
L'honorable Allan Rock, C. P., député, ministre de l'Industrie  
V. Peter Harder, sous-ministre de l'Industrie  
Nicole Jauvin, sous-solliciteur général  
Morris Rosenberg, sous-ministre de la Justice

**Ministerial Correspondence Unit / Unité de la Correspondance Ministérielle**  
**Routing Slip / Feuille de controle**

Letter/Lettre Date: 2002-11-01

s.19(1)

**Author/  
Auteur:**

President and Chief Executive Officer  
Canadian Wireless Telecommunications  
275 Slater Street, Suite 500  
Ottawa ON  
K1P 5H9

**Document: 2002-023193**

**Doc Type/Type de Doc: D**

**File / Classer: 270201**  
**CANADIAN HERITAGE - GENERAL**

**Referred To/Transmis a: MCUED3**

**Date: 2002-11-15**

**Due Date/Date d'échéance: 2002-12-13**

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

**Additional Comments / Remarques additionelles:**

**CC:**  
**CC:**

**CC:**  
**CC:**

**CC:**  
**CC:**

**CC:**  
**CC:**

**Closed / Fermer:**

**File Away / Classer:**

**Description of type / Description des types**

D: yellow docket / dossier jaune (draft response / projet de réponse)

A: further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

follow-up at your discretion / donner suite à votre discrétion

for your information (no action required) / à titre d'information (aucune mesure requise)

November 1, 2002

The Honourable Martin Cauchon, P.C., M.P.  
Minister of Justice  
and Attorney General of Canada  
Department of Justice Canada  
284 Wellington Street  
Ottawa, Ontario  
K1A 0H8

Dear Minister:

**Re: Lawful Access Consultation**

On behalf of the Canadian Wireless Telecommunications Association (CWTA), I am writing to you today in regard to the Lawful Access consultation document issued by the Department of Justice Canada, Industry Canada, and the Solicitor General Canada on August 25, 2002. I believe that the results of the consultation will be improved through the provision of additional details.

On October 15, 2002, CWTA members had the opportunity to participate in a bilateral meeting with officials from the three above mentioned departments. While these officials have been helpful in clarifying a number of points in the consultation document, a number of critical questions remain unanswered.

We suggest that draft legislation as well as any accompanying regulations should be provided for public consultation. While we would expect an opportunity to comment on the draft legislation during the usual Parliamentary process, it is equally important, in our view, to have a full and complete opportunity to comment on any proposed draft regulations and any accompanying standards associated with the proposed legislation.

.../2

2/...

In order to provide meaningful comment on the policy proposal, service providers must understand the requirements that they will be expected to meet under the new proposal. We understand that these requirements will be detailed in the new regulations. Neither the requirements, nor the regulations, have been provided to the members of the CWTA for their consideration and comment.

Further, some of the key elements of the proposal have not been defined. For example, the proposal states that all service providers must have a "basic intercept capability". Similarly, the proposal states that service providers will be expected to assume the cost of providing lawful access capabilities whenever they undertake a "significant upgrade". In both cases, definitions have not been provided for these terms.

CWTA recognizes that lawful access is an essential tool for national security and law enforcement. We would like to provide constructive comments regarding the proposal but our ability to do so will be limited unless further details, such as suggested above, are provided.

We look forward to reviewing the additional information and to provide constructive comments in this important consultation process. s.19(1)

If you or your officials require further assistance, please do not hesitate to contact [redacted] Vice-President Industry & Regulatory Affairs, at (613) 233-4888 ext. [redacted] or myself.

Yours sincerely,

Cc: The Honourable Wayne Easter, P.C., M.P., *Solicitor General*  
The Honourable Allan Rock, P.C., M.P., *Industry Canada*  
V Peter Harder, Deputy Minister, *Industry Canada*  
Nicole Jauvin, Deputy *Solicitor General*  
Morris Rosenberg, Deputy Minister, *Justice Canada*

s.19(1)

President and Chief Executive Officer  
Président et chef de la direction

Le 1<sup>er</sup> novembre 2002

L'honorable Martin Cauchon, C. P., député  
Ministre de la Justice  
et procureur général du Canada  
Ministère de la Justice  
284, rue Wellington  
Ottawa (Ontario) K1A 0H8

**Objet : Consultation sur l'accès légal:**

Monsieur le Ministre,

Je vous écris suite à la consultation amorcée par la publication du document conjoint des ministères de la Justice, de l'Industrie et du Solliciteur général sur l'accès légal, le 25 août dernier et ce, au nom de l'Association canadienne des télécommunications sans fil (ACTS). Nous croyons que cette consultation sera plus productive si on fournit plus de détails aux intéressés.

Le 15 octobre, les membres de l'ACTS ont eu l'occasion de rencontrer des fonctionnaires des trois ministères susmentionnés. Bien que ces représentants aient aidé à éclaircir divers points du document de consultation, il en reste d'autres, d'importance critique, à propos desquels des questions subsistent.

Tout projet de loi modifiant la législation sur l'accès légal et tout règlement en découlant devrait, à notre avis, faire partie de la consultation publique. Bien qu'il soit vrai que nous aurons sans aucun doute la possibilité de présenter des observations sur un tel projet dans le cadre normal de la procédure parlementaire, il nous semble tout aussi important d'avoir la possibilité de le faire, de manière aussi complète, au sujet de tout projet de réglementation et de norme dont s'assortirait le projet de loi.

Pour contribuer de façon vraiment utile à l'examen de la politique proposée, nos membres doivent saisir toute l'ampleur de ce qu'on attendrait d'eux selon cette proposition. On nous dit que ces exigences seront détaillées dans les nouveaux règlements. Toutefois, aucun projet de règlement ni énoncé des exigences qu'il comportera n'a été mis à notre disposition pour que nos membres et nous puissions l'étudier et présenter des observations.

.../2

2/...

De plus, certains des éléments clés de la proposition ne sont pas définis. Par exemple, il y est dit que tous les fournisseurs de services de télécommunications seraient tenus d'assurer au moins une « capacité de base d'interception ». Il y est dit également que ces fournisseurs devraient supporter le coût de l'accès légal en cas d'« amélioration significative » de leur système ou réseau. Or, ni l'une ni l'autre de ces expressions n'est définie.

Nous reconnaissons que l'accès légal est un outil indispensable pour les responsables de la sécurité nationale et de l'application de la loi. Nous souhaitons présenter des observations constructives concernant la politique et le projet envisagés, mais nous pourrions difficilement le faire à moins qu'on ne nous fournisse le genre de détails susmentionnés.

Nous avons hâte de nous pencher sur ces renseignements afin de pouvoir faire un apport éclairé à cette importante consultation.

Si vos fonctionnaires ou vous-même avez besoin de plus de précisions sur les renseignements qui nous semblent nécessaires, veuillez ne pas hésiter à communiquer avec notre vice-président aux affaires réglementaires et de l'industrie, [REDACTED] que vous pouvez joindre au (613) 233-4888, poste [REDACTED] ou avec moi.

Avec mes remerciements anticipés, je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma très haute considération.



s.19(1)

c.c. : L'honorable Wayne Easter, C. P., député, solliciteur général  
L'honorable Allan Rock, C. P., député, ministre de l'Industrie  
V. Peter Harder, sous-ministre de l'Industrie  
Nicole Jauvin, sous-solliciteur général  
Morris Rosenberg, sous-ministre de la Justice

b.c.c: Paul Pierlot, conseiller principal, ministère de la Justice

**Cloutier, Marie**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Nov 01 7:08 PM  
**To:** la-al@justice.gc.ca  
**Cc:** Clark, Joe - M.P.  
**Subject:** Lawful Access Consultation,

I am writing to express my concern on the reduction of the rights and freedoms guaranteed in the Canadian Charter of Rights and Freedoms, particularly the right to be secure against unreasonable search and seizure. It would appear to me when reading the materials provided on the [www.canada.justice.gc.ca/en/cons/la\\_al](http://www.canada.justice.gc.ca/en/cons/la_al) site that in order to meet the terms of a treaty established outside of Canada and without consultations with Canadians, that we will be extending the ability of Canadian law enforcement to build a "big brother" society where they will be able to monitor Canadians at will with little or no oversight by the courts.

This to me is unacceptable. While I am behind the Law Enforcement establishments goals to protect Canadians from wrongful acts, I do believe that there needs to be oversight by the courts in the implementation of monitoring of our citizens. The use of "production orders" and "assistance orders" seems to be circumventing the concept of a search warrant.

To quote the document: "The *Criminal Code* generally provides that law enforcement agencies cannot obtain documents or information without having reasonable grounds to believe that an offence has been or will be committed. This requirement is a safeguard that balances the state's need to obtain evidence of a crime with the privacy interests of a person holding information. This requirement is particularly appropriate where there is a high expectation of privacy, such as in regard to the content of a private document."

It then goes on to state that there is not a "high expectation of privacy" in relation to internet technologies, with highlights on "e-mail". While it may be technically trivial to obtain an e-mail that is in transit or stored on a hard drive at an ISP, or a user's computer, I am sure that if a poll was taken of "average" internet users, it would be found that many if not all of them expect that the e-mails they send would be as private as a letter that they have written and mailed with a stamp, or a conversation that is spoken over the telephone. It is also "technically trivial" to open postal mail, but I do believe (or at least hope) that law enforcement officials are not able to open a person's correspondence without first obtaining a warrant.

I strongly believe that there should be judicial and/or public oversight of law enforcement agencies requesting the ability to monitor Canada's citizens. The ability for me to send you this letter stating my opinions on this matter without the worry that this communication would be monitored by law enforcement is fundamental part of being Canadian, and living in a free society. Please ensure that our rights as Canadians are not degraded by implementing the suggestions in this paper.

Rob

[REDACTED]  
Pandell Technology Corporation  
[REDACTED]

**Cloutier, Marie**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Nov 04 3:17 PM  
**To:** la-al@justice.gc.ca  
**Subject:** lawful access consultation timeframe extended?

Hello,

Could you please tell me the final date for submissions on the consultation on Lawful Access?

The canada.justice.gc.ca website says "November 15, 2002" but several agencies have stated the deadline has been extended to December 15, 2002.

Is that correct? What is the final date for submitting on this topic?

Thank you

[REDACTED]

2002-12-11

000132



erek Egan - Lawful Access Consultation

RECEIVED BY MAIL NOV 4, 2002

From: [REDACTED]  
To: la\_al@justice.gc.ca  
Date: 10/31/02 11:12am  
Subject: Lawful Access Consultation

THIS ADDRESS IS INCORRECT

s.19(1)

Thank you for the opportunity to comment on the issue of lawful access. In short, the proposals as contained in the consultation document are sound. We understand this to be a "work in progress" and expect that we will be notified of further developments.

[REDACTED]  
Saanich Police  
760 Vernon Avenue  
Victoria, BC, V8X 2W6  
Telephone: (250) 475 4322

CC: [REDACTED]

**Cloutier, Marie**

---

**From:** [REDACTED]  
**Sent:** 2002 Nov 05 10:52 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Having read the following document

s.19(1)

<http://news.com.com/2100-1023-955595.html> Will Canada's ISPs become spies

I am appalled that Canada is considering such a thing. I thought Canada was the land of freedom.

Cloutier, Marie

---

From: [REDACTED]  
Sent: 2002 Nov 06 6:53 AM  
To: Sheila Copps; la-al@justice.gc.ca  
Subject: Internet Eavesdropping Proposals

s.19(1)

I Am Sorry -

I strenuously object to any adoption in secret or in public of Justice's internet privacy study and the very fact of its commissioning makes any Liberal denial of implementing it less than credible (remember the GST?). This study alone will cost the Liberal party federally many, many votes.

Even outgoing Alexa McDonald knows enough to challenge CCRA's disability tax credit grab. It is too late to reverse the rebirth of Revenue Canada's feudal reach as the new CCRA, but the new retraction of on-demand "C-Screen Printouts" affects everyone on a means-tested income. I am afraid the prediction for the coming election is a challenge for the Liberals to maintain their sweeping lead.

[REDACTED]

---

Bolt. Everything you need to speak your mind, hang out, hook up ... whatever. Tagbooks <sup>TM</sup>, Bolt Notes <sup>TM</sup>, message boards, personality quizzes, photos, free stuff and lots more! <http://www.bolt.com>

**Cloutier, Marie**

---

**From:** [REDACTED]  
**Sent:** 2002 Nov 06 11:46 AM  
**To:** la-al@justice.gc.ca  
**Subject:** Lawful Access Consultative Process

s.19(1)

Hi,

VeriSign, Inc. is planning to submit comments in the consultative process in the next few days.

We did wish to check, however, whether the comments will be available to the public or not. We would strongly prefer the latter due to the nature of the topic.

sincerely,

[REDACTED]

[REDACTED]

NetDiscovery Strategy  
VeriSign, Inc

[REDACTED]

Dulles VA  
USA  
tel: +1 703.948.4305

Cloutier, Marie

---

From: [REDACTED] s.19(1)  
Sent: 2002 Nov 06 2:14 AM  
To: la-al@justice.gc.ca  
Subject: Comment submission re: Lawful Access consultation



ACCESS.TXT

File attached is my comment to the consultation document regarding  
lawful access at [http://www.canada.justice.gc.ca/en/cons/la\\_al/index.html](http://www.canada.justice.gc.ca/en/cons/la_al/index.html)

My contact information

[REDACTED]  
[REDACTED]  
Toronto, Ont  
[REDACTED]

## Preamble

=====

Upon reading the document, I notice with dismay that while there are five references in the text to the Canadian Charter of Rights, and seven references to the Council of Europe. The Council of Europe requires this, the Council of Europe requires that, the Council of Europe requires the other. The recommendations in the consultation document may or may not be good ideas, but they should stand or fall on their own merits. Canada is an independent country. If the document has to resort to what foreign countries several thousand miles away are doing as justification, that is a prima facie indication that ideas presented in the document fail to stand on their own merits.

You will probably receive a number very strongly-worded submissions on these proposals, some bordering on outright hatred. I would like to point out the context engendering this sentiment. The well has been poisoned by a very similar discussion paper, put out by the CRTC a few years ago. The CRTC is seen by some segments of the Canadian public as a bunch of fanatical, Ameri-phobic, control-freaks, whose goal in life is to build an electronic Berlin Wall at the 49th parallel.

Soon after assuming the Chair of the CRTC, Mme. Francoise Bertrand made public statements to the effect that Canadians were spending too much time at American websites, and by golly we're going to do something about it. Some time afterwards, came a discussion paper about regulating the internet in Canada, to an extent that only totalitarian regimes attempt nowadays, in the name of protecting children and

## Access

fighting crime. It was a very blatant power-grab aimed at virtual ly shutting down international internet access, and then rationing out access only to government-approved sites. People asked very pointed and embarrassing questions about why the CRTC was jumping into criminal law enforcement. The CRTC's ideas, which could be used as a template for current Chinese internet censorship were, thankfully, abandoned.

The current discussion document uses virtually the same justifications (child-porn and other criminal activity) as the CRTC document. The sense of déjà-vu is very strong. This time at least, the Department of Justice actually has jurisdiction in the areas used as justification to intervene, but you are dealing with a very cynical public which will see many parallels with the previous discussion paper, and consider this to be merely phase 2 of the original attack on internet access launched by the CRTC.

Part 1) Financial impacts on ISPs/individuals other than mega-ISPs  
=====

The document seems to have been written by a bureaucratic mindset that is accustomed to dealing only with other large bureaucracies. The reporting and other red-tape in the recommendations may be bearable by a large mega-ISP like Sympatico, AOL, Rogers, or MSN. Because these recommendations seem tailor-made strictly for mega-ISPs, I fear that the costs and regulatory burdens they impose would financially destroy

## Access

smaller "mom 'n pop" operations. My concern is that this would lead to an oligopoly of mega-ISP's that could charge extortionate rates, because there would be no low-cost competition. Consider...

- In my case, I subscribe to a small ADSL ISP that currently (November 2002) charges \$29.95/month including a base amount of 15 gigabytes of traffic (combined up+down loading) on circuits capable of just over 1 megabit/second download. Excess usage is \$3/gigabyte.

- For similar speeds, Bell Sympatico charges \$44.95/month and \$7.95 per gigabyte for excess traffic beyond a base amount of 10 gigabytes.

I normally use less than 2 gigabytes/month. Even so, Sympatico would cost me 50% more.

Another problem with mega-ISP's is that they dumb down their service to the AOL level. This means not offering static IP addresses or allowing hobbyists to run public servers. I realize that there are many unsophisticated users out there who merely want to surf and use email, with the least difficulty. We were all beginners at one time, and I don't begrudge beginners the right to a "user-friendly" ISP with training wheels. What I'm unhappy with is the prospect of AOL/MSN or similar service being rammed down my throat once the small independents are forced out of business. There's a world of information out there on the internet. I don't want to spend my online time in an "electronic shopping mall" or a "portal", which mega-ISP's would like to confine me to.



## Access

There are also small specialised service providers who provide web and domain hosting to small businesses at reasonable prices. They are an alternative to big providers who are geared to serving big businesses at big-business rates, i.e. totally unaffordable to small business.

To protect the smaller service providers from bankruptcy by costs of regulation, I propose that the authorities bear all costs of installing extra technology. Even better, records/logs could be forwarded in real time to large arrays of servers maintained by law-enforcement agencies. If they find this data too much to handle/store, how can they ask this of small businesses ?

As for operational assistance, I suggest the rate schedules in the FOIA (Freedom of Information Act) as the basis for calculating compensation. This is what the government charges when the public demands that the government dig up records/information. It would be hypocrisy not to apply the same standards to government demands for information from the public.

I also fear that the overly broad definition of "Service Provider" means that a hobbyist who runs a small website or other public server from their home would be saddled with the same regulatory burdens as a multi-billion dollar outfit like BCE or Rogers. A home hobbyist should not have to worry about... "the competence, reliability and deployment of employees."

### Part 2) Potential impacts on spam-filtering

A list of circumstances under which interception is allowed implies

Access

that interception is not allowed in any other circumstances. That raises questions about virus scanners/blockers as well as spam filters and boycotts of traffic from spam-supporting ISPs. Therefore I urge that service providers be authorized to block incoming malicious communications, including but not restricted to email, worms, DOS (Denial Of Service) attacks, and probes that may be used to facilitate attacks against a computer or network.

The subject of spam is worthy of a treatise in its own right. I will restrict myself here to impacts of the proposed legislation. What many internet users dread is the day that mainstream advertisers start using spam as an advertising method. AOL might have had the millions to fight off Sanford Wallace in court. Will small ISP's be able to fight off lawsuits from multi-national corporations with billions in their coffers, demanding access to users' inboxes? As an internet user I've seen it all. Every spammer seems to claim the \*THEIR\* email isn't spam; it's a "targetted e-mailing" containing "important information" and "exciting offers". And if claiming that their spam is a "private communication" can make blocking the spam illegal, they will resort to it.

Rejecting email from a wide-open email relay that is being heavily (ab)used by spammers not only blocks the 99% that is spam, but also blocks the 1% legitimate email. Additionally, in some cases, the only way to apply pressure on spammers and the ISPs who supply their bandwidth is via boycotts including the rejection of all traffic from the offending ISP, and possibly their upstream provider. This is especially true where a spamming customer of an ISP incorporates a dummy ISP, and their former ISP becomes an "upstream provider" to

Access.

the  
spammer. The shell game doesn't really change anything except on  
paper.

I wish to emphasize that the internet is a network of privately-  
owned  
networks. The private networks are private property and advertise  
rs  
have no more right to force their way into my inbox than a salesma  
n has  
to kick in the door and force his way into my home.

I urge that provision be explicitly made in the legislation to a  
llow  
interception/blocking of any data-packets, including but not restr  
icted  
to email, by an ISP regarding any traffic destined to its network.

And  
that senders have no recourse in law against such blocking carried  
out  
by ISPs. Given the rapidity with which spammers' tactics evolve,  
ISPs  
should \*NOT\* have to wait for an act of Parliament each time spamm  
ers  
find a new trick. End-users should be notified of their ISP's pol  
icies  
and practicies regarding such blocking.

Part 3) Will this really accomplish the publicly stated goals ?  
=====

Certainly not enough to justify the expense and time and disrupt  
ion  
and loss of privacy caused by the necessary implementations. That  
, in  
the final analysis, is the strongest, most telling argument agains  
t the  
proposals. Internet monitoring will \*NOT\* catch determined terror  
ists.

I wish to draw people's attention to the following article on the  
CNN  
website  
<http://www.cnn.com/2001/US/09/20/inv.terrorist.search/index.html>  
Especially the passage...

> Simon Reeve, the author of "The New Jackals: Ramzi Yousef, Osama  
> bin Laden and the Future of Terrorism," says bin Laden has ditch

ed  
> his satellite-linked phones, mobile handsets and Internet access  
in  
> favor of "Stone Age" messaging techniques to elude law enforcement.  
>  
> "Bin Laden is not now using any sophisticated communications  
> technology," the London-based Reeve says.  
>  
> "The American National Security Agency has devoted huge resources  
s  
> trying to trace him through his old satellite and portable phones,  
s,  
> but he no longer uses them, to avoid being targeted and attacked  
."

In the initial stages, internet traffic spying will catch a few  
\*VERY\*  
stupid/naive criminals. But once it gets pounded into people's heads  
that any data packets you send out from your computer may be used  
against you in court and end up in the newspapers, people will clamor  
up,  
and conviction rates will soon fall to previous levels. Given falling  
long-distance rates, and the fact that much of Canada's population  
lives  
near the US border, dialing up to an ISP just across the border is  
very  
feasible. Furthermore, there is very strong encryption available  
to  
the  
public. Before anyone proposes outlawing strong encryption, let me  
point out that...

- someone who is willing to kill people, produce child pornography,  
etc, will not likely be deterred by one more charge of using  
illegal  
encryption.

- steganography, the art of concealing communications in innocent  
looking files/transactions, renders decryption abilities moot.  
It  
is not even obvious that there's any encrypted traffic to decrypt

ypt.

To summarize, law-enforcement will see little benefit. If the recommendations are put through in their present form, Canada will be a less-connected society, paying much more for internet access to fewer ISPs, specifically mega-ISPs. The cynical side of me, and many other Canadians, will see that as the real goal of these recommendations.

My recommendations are as follows...

- all costs of monitoring to be picked up by government.
- ISPs will not be required to hire additional staff.
- I have no objection to logs/records being forwarded in real-time to government-owned servers, as long as all associated costs come out of general revenue.
- revised legislation regarding interception/blocking be worded so as not to interfere with data-traffic blocking/boycotts carried out by ISPs.

**Cloutier, Marie**

---

**From:** [REDACTED] **s.19(1)**  
**Sent:** 2002 Nov 07 3:23 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Lawful Access Consultative Proceeding: Comments of VeriSign, Inc



Comments\_VeriSign\_fi  
nal.doc

VeriSign hereby conveys its comments in  
the subject proceeding.

[REDACTED]  
Vice President  
NetDiscovery Strategy  
VeriSign, Inc  
mailto:[REDACTED]  
mob: +1 703.887.5196  
Office:  
21345 Ridgetop Circle  
Dulles VA 20166-6503  
USA  
tel: +1 703.948.4305

*Before the*  
Department of Justice  
Industry Canada  
Solicitor General Canada  
Criminal Law Policy Section  
284 Wellington St.  
Ottawa, ON K1A 0H8

*In the matter of:* | Lawful Access - Consultation Document  
| of August 25, 2002  
| Legislative Proposals

**Comments of VeriSign, Inc.**

**1. Introduction**

VeriSign, Inc (VeriSign) is a globally-recognized provider of trusted infrastructure signalling and authentication services in the telecommunication, Internet, and financial services sectors. It also provides an array of Lawful Interception (LI) services (i.e., Lawful Access) on a large-scale. This includes a commercial service bureau offering for communication service providers - as a means for them to meet their national LI capability obligations, and Law Enforcement Agencies as a "one-stop" means of implementing intercepts. These services are collectively referred to as VeriSign NetDiscovery™ Service.

Headquartered in Mountain View, California, VeriSign has facilities at nearly 100 locations in the United States, and in a dozen different countries; combined with thousands of affiliate providers of its services worldwide.

VeriSign has also taken an active role in participating and contributing in multiple LI technical development, industry collaboration, standards, and governmental advisory organizations and functions worldwide. This includes creation of a sector trade association, the Global LI Industry Forum. See [WWW.GLIIF.ORG](http://WWW.GLIIF.ORG)

VeriSign believes its experience in providing innovative low-cost intercept capability solutions to communication service providers is directly relevant to this consultative proceeding. We commend the Department of Justice, Industry Canada, and the Solicitor General for undertaking the proceeding and appreciate the opportunity to submit these comments. For improved reference, the same structure as the consultative document has been maintained, with the relevant document text shown.

## 2. Infrastructure Capability

### 2.1 Requirement to Ensure Intercept Capability; General Requirements

It is proposed that all service providers (wireless, wireline and Internet) be required to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies.

The central tenet of the proposal is that service providers would be required to have the technical capability to provide access to the entirety of a specific telecommunication transmitted over their facilities, subject to a lawful authority to data associated with that telecommunication.

A new law addressing the requirement for service providers to have intercept-capable transmission apparatus could set out the following:

- general operational requirements describing the interception capability;
- regulation-making authority to specify the details of the functional requirements;
- a capacity for forbearance from certain obligations; and
- a compliance mechanism.

#### General Requirements

The legislation would apply to all service providers operating a telecommunications facility in Canada. All service providers would be required to provide, at a minimum, a basic intercept capability before providing new services or a significantly upgraded service to the public.

Such intercept capabilities are fully consonant with requirements in nearly every country, as well as mandated by the Council of the European Union.<sup>1</sup> Standards making activities to implement these requirements have been effected in many countries. Substantial global coordination and harmonization of technical standards occurs in the Lawful Interception Technical Committee (TC LI) of the European Telecommunication Standards Institute (ETSI).<sup>2</sup> Global coordination of LI legal information schema has also recently been initiated in the LI-XML Technical Committee of the Organization for the Advancement of Structured Information Standards (OASIS).<sup>3</sup>

VeriSign has demonstrated with its NetDiscovery™ commercial service offering that existing capability requirements can be provided efficiently and very cost-effectively for all communication providers by using a service bureau. The technical systems, security office, administrative, and personnel costs are thereby shared among a large number of service providers (wireline, wireless, internet, cable). If properly designed and implemented, the services through a service bureau approach provide greater security and authentication, as well as more cost-effective and a timely solution for law enforcement agencies.

<sup>1</sup> 496Y1104(01), Council Resolution of 17 January 1995 on the lawful interception of telecommunications, *Official Journal C 329*, 04/11/1996 p. 0001 - 0006

<sup>2</sup> See [www.etsi.org](http://www.etsi.org)

<sup>3</sup> See [www.oasis-open.org](http://www.oasis-open.org)



## 2.2 Regulations

The legislation would set out the definitions and the general approach and would provide authority for the Cabinet, on the advice of the Minister of Industry and the Solicitor General, to make regulations within the authority provided in the statute. Technical standards and details could be specified in the regulations.

The scope of the regulations is open to discussion but could include authority relating to the setting of technical and other standards or requirements for a service provider. Regulations could describe what service providers must do to provide access to their facilities, security requirements relating to how intercepted information is handled, issues related to costs, and the manner in which the regulations are to be developed.

Here also, this general approach and delegation of authority is the practice followed worldwide. It is the practice in many jurisdictions, however, to eschew the inclusion of detailed technical standards in the operative regulations. Telecommunication, Internet, On-line services and LI technologies are constantly evolving. Multiple industry standards forums already exist to create and maintain LI standards – some on a global basis. The providers of LI products and services typically design their offerings to meet these industry standards. For these reasons, it would be very difficult and essentially unnecessary for Canada to develop yet another set of technical standards and include them in the form of regulations.

A regulatory requirement for communication providers to meet established industry standards through some formal certification process with attendant penalties for noncompliance seems like the best approach for all concerned.

## 2.3 Forbearance

One mechanism to provide flexibility and avoid problems such as the creation of "intercept safe-havens" would be a system of forbearance. This forbearance would remove the obligation to comply with the requirements of the statute or regulations, in whole or in part, for a limited time.

Given the feasibility of providing these capabilities easily and cost-effectively through a service bureau, it is not apparent that a general forbearance policy is needed or appropriate. Intercept solutions presently exist for essentially all production public telecommunication, Internet, and On-line service offerings today.

Some consideration, however, may wish to be given to a forbearance policy for highly experimental new services implemented on a small scale, for private closed user group networks (e.g., Intranets). It seems unnecessary if not infeasible to impose general public communication provider LI requirements on such implementations.

## 2.4 Compliance mechanism

Provisions for monitoring compliance would help ensure that the legislation is effective and that service providers have a mechanism to help ascertain compliance with the law. The provisions could authorize or require inspections or analyses to be conducted. However, these mechanisms would need to minimize the costs for both industry and government.

Issues to be considered

- what kind of compliance mechanism should be established?
- who should conduct the compliance activities and prescribe the circumstances under which they may be conducted?
- what type of penalty should be provided for in cases where service providers do not comply with the law?

In most jurisdictions worldwide, compliance with LI requirements is achieved through self-certification processes. In other words, the communication provider, under some significant penalty for noncompliance, provides notice to a central national bureau that the required capabilities have been implemented. This requirement also typically includes an essential component – namely the central bureau subsequently providing the LEAs who will make use of this service, the local or service bureau contacts are for executing a warrant for intercept capabilities.

Where a communication provider chooses to outsource the both the compliance requirements and the execution of warrants to a service bureau, the bureau typically undertakes the self-certification process and acts as the communication provider's agent in all LI matters. This mechanism drastically reduces the cost of on-going compliance monitoring for each service provider and provides an independent 3<sup>rd</sup> party that can provide additional due diligence and scrutiny to the service provider compliance.

## 2.4 Costs of Ensuring Intercept Capability

1. service providers would be responsible for the costs associated with providing the lawful access capability for new technologies and services, and
2. service providers would be responsible for the costs associated with providing a lawful access capability when a significant upgrade is made to their systems or networks, however
3. they would not be required to pay for necessary changes to their existing systems or networks.

The costs associated with ensuring intercept capabilities fall into multiple categories: 1) access devices, including hardware/software modifications to existing systems, 2) mediation devices that cause the access devices to effect the interceptions pursuant to warrants and deliver the evidentiary material to law enforcement monitoring facilities, 3) LI-related circuits for connectivity between a service provider and an LEA, 4) security office, including legal and regulatory, 5) administration of warrants, including authentication and backwards compatibility with legacy judicial practices, and 6) personnel and training.

National authorities have typically taken one or a combination of two approaches to implementing intercept capabilities – a) encumber service providers with LI costs that are reflect back in the cost of service to customers, or

b) reimburse providers for costs incurred. There is both an "up-front" capability component, as well as a continuing "as needed" set of costs. The reimbursements are variously applied (or not) to one or more of the above six cost categories.

Most contemporary public telephony switches, including Internet softswitch equivalents, by virtue of established LI national requirements and associated standards for intercept capabilities, are already capable of supporting existing LI standards. For these switches, communication service providers should not be encumbered with significant upgrade costs.

Some older switches, as well as most ISP facilities, require some form of adjunct Access Device – for which there are associated costs. For this equipment, Canadian communication service providers should be able to take advantage of shared capabilities through a common service bureau where the development costs are spread across a large number of providers.

For all providers, for all non-technical capability requirements, dramatic cost savings are similarly possible through the use of a service bureau approach through consolidation and sharing of administrative activities, security offices, and other resources among communication providers, and a "one-stop" mechanism for LEAs.

VeriSign makes no comment on which reimbursement approach is appropriate for Canada, except that whatever choice is made, allowance be made for a Service Bureau acting as agent for carriers and enjoying standing to obtain reimbursements. This would encourage a result that saved substantial overall costs for Canada and Canadian citizens.

S. 20

### 3. Amendments to the Criminal Code and other statutes

#### 3.1 Production orders; General production orders

VeriSign makes no comment.

#### 3.2 Specific production orders

"Telecommunications Associated Data" means any data, including data pertaining to the telecommunications functions of dialling, routing, addressing or signalling, that identifies, or purports to identify, the origin, the direction, the time, the duration or size as appropriate, the destination or termination of a telecommunication transmission generated or received by means of the telecommunications facility owned or operated by a service provider.

A specific production order could be created under a lower standard in order to allow for the production of telecommunications associated data, that extends beyond the telephone numbers already covered by section 492.2 of the Criminal Code, historic traffic data or real-time collection of traffic data. Although real-time search of traffic data is already permissible under either section 487.01 or Part VI, the standard for Internet traffic data should be more in line with that required for telephone - records and dial number recorders in light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication. A specific production order to be issued under a lower standard could also be created to obtain other data or information in relation to which there is a lower expectation of privacy.

##### Issues to be considered

- should there be a specific power, parallel to that provided for in the Criminal Code dial number recorders, to allow law enforcement and national security agencies to obtain traffic data?
- how should "traffic data" be defined? Should the definition of traffic data be combined with telephone-related information and addressed in the same Criminal Code provision?
- should other specific production orders be created under a lower standard?
- what kind of procedural safeguards should be included? (e.g., s. 487) because law enforcement agencies may require the information for they are at the early stages of an investigation.

In most countries, a significantly lower burden on LEAs is imposed for obtaining Telecommunications Associated Data, including data relating to Internet services. Indeed, globally, this is referred to as Intercept Related Information (IRI), and a specific HI2 interface has been developed in ETSI. It provides a good fit for the application of Telecommunications Associated Data requirements to complex new service environments, including Internet-based ones.<sup>4</sup>

Recent initiatives have been established in the ETSI Lawful Intercept Technical Committee to specifically deal with IRI associated with Internet access and Internet mail

<sup>4</sup> "intercept related information: collection of information or data associated with telecommunication services involving the target identity, specifically communication associated information or data (including unsuccessful communication attempts), service associated information or data (e.g. service profile management by subscriber) and location information." ETSI Standard, **Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecommunications traffic**, ETSI ES 201 671 V2.1.1 (2001-09) at 13.

services. The capabilities are actually available today, but not standardized on a global basis among all LI product and service providers. Canadian law enforcement and national security agencies should certainly have access to this IRI information, subject to appropriate judicial safeguards, and any contemplated "traffic data" definitions should be made consonant with the global IRI terms and definitions. The collection and archiving of "traffic data" can be accomplished on a network-wide basis through a centralized service bureau which can further provide services to allow authorized and authenticated access to various part of the collected/archived information per legal authority of a search warrant or production order.

VeriSign takes no position on specific procedural safeguards other they be made flexible to accommodate exigent circumstances and be cable of being expressed in the new LI-XML legal information exchange formats to expedite and authenticate the submission and handling of judicial warrants.

### **3.3 Orders to obtain subscriber and/or service provider information; Assistance orders**

VeriSign makes no comment.

### **3.4 Data-preservation orders**

A preservation order could require an Internet service provider (ISP) not to delete specific existing information relating to a specific subscriber. It is meant as a stop-gap measure to ensure that information vital to a particular investigation is not deleted before law enforcement officials can obtain a search warrant or production order. Consideration also needs to be given to exigent circumstances, situations in which it could be argued that law enforcement agencies should be able to impose on a service provider the requirement to preserve data even without a judicial order for a specified period such as four days, if the conditions for obtaining a judicial order exist but it would be impracticable to obtain one. An exigent circumstance provision is already included in the Criminal Code in relation to search warrants and wiretaps.

It should be noted that data preservation is different from data retention. Data preservation, as outlined above, involves serving a judicial order on a service provider to ensure that existing specified information in relation to a particular subscriber is not deleted. Data retention, however, is a general requirement that could compel service providers to collect and retain a range of data concerning all of its subscribers.

#### **Issues to be considered**

- should a data-preservation order apply only to stored computer data or should it also apply to paper records?
- under what legal standard should a data-preservation order be granted?
- should standards vary depending on the nature of the data?
- who should be authorized to issue a preservation order?
- what is a reasonable period for a custodian of data to be compelled to preserve data: 90, 120, 180 days?
- should there be a specific penalty for non-compliance with a preservation order, or is contempt of court sufficient?
- for how long should a law enforcement official be able to impose a preservation order on service providers in exigent circumstances?

VeriSign takes no position on these issues. However, it is worth noting that the cost of storing exceedingly large amounts of data had decreased by orders of

magnitude over the past decade on both magnetic and optical media. For normal system management, backup, and restoration purposes, it is not unusual for Internet and On-line service providers to store substantial amounts of subscriber data for long periods of time. VeriSign NetDiscovery™ Service offers archival periods of several years. Additionally, the entire concept of a communication identifier in a converged media environment with agile access and services has evolved into that of a "signature." In this environment, it will be essential to archive and intelligently search for a target signature if law enforcement and national security agencies are to be even aware of a suspect's communications activity.

### **3.5 Virus Dissemination**

VeriSign makes no comment.

### **3.6 Interception of e-mail**

- should there be a specific provision in the Criminal Code in relation to how an e-mail should be acquired?
- if such a provision should be included, what kind of procedural safeguards should be imposed?
- should the type of order to be obtained in order to acquire an e-mail vary depending on the stage of the communication or delivery process?

As noted above, it seems generally inadvisable to include intercept methodology details in organic law. E-mail is one of a species of interrelated messaging capabilities available to users. Both e-mail and related intercept technology - not to mention the very concept of e-mail - is evolving rather quickly. The ETSI Lawful Intercept Technical Committee has just established a working group devoted exclusively to preparation of global specifications related to e-mail - which should be useful in dealing with this matter.

There is no apparent reason why e-mail could not be treated like any other form of communication - divided into basic customer account information, communication record detail, Intercept Related Information, and communications content. In most jurisdictions, the first generally requires little or no procedural action, while remaining actions require increasingly greater levels of probable cause and judicial review.

The type of order would seem related to the nature of the data or content being acquired, rather than the stage of the communication or delivery process. This approach would also allow treatment of all user services in a similar fashion.

### **3.7 Amendments to the Competition Act**

VeriSign makes no comment.

#### **4. Other mechanisms to provide subscriber and service provider information**

- what type of mechanism, if any, should be put in place to provide law enforcement and national security agencies with up-to-date and accurate CNA and LSPID information while respecting the privacy of Canadians?
- should an obligation to collect such CNA information be imposed even if the service provider does not collect this information for its own purposes? In other words, should a provider be compelled by law to collect CNA information?
- some mechanisms with respect to CNA information are already in place with respect to telephones. Should such mechanisms be created or adapted to provide similar subscriber information for Internet service providers?
- who should pay the costs of collecting, retaining and accessing this information?
- if a database were to be established, who should operate this database?

VeriSign through its Illuminet subsidiary has had many years of experience in providing Customer Name and Address (CNA) and Local Service Provider Identification (LSPID) information in the USA, although the extant regulations, tariffs, and operating arrangements are somewhat different in Canada.

The timely, accurate provisioning of CNA and LSPID information is critical to law enforcement and national security agencies in effecting lawful intercepts, and should be made available for their use with minimal or no impediments on a protected basis. This information seems so basic to operating a legitimate business, that imposing an obligation to collect CNA should represent no significant burden whether a telephone services provider or an ISP.

In most jurisdictions, LEAs pay for access to and delivery of this information on commercial terms.

A single central database seems infeasible and unneeded. This reference information can be provided through a combination of contemporary data exchange standards combined with access arrangements to effect interoperability among database systems.

On the other hand, what is very attractive for this purpose is the establishment of a central clearinghouse for this kind of information – either as specially appointed by the Federal government, or offered as a commercial service to law enforcement and national security agencies. VeriSign is offering the latter capability today as part of its NetDiscovery™ Service.

As part of the ongoing consultative process, VeriSign would be pleased to provide additional information or meet with the agencies and staff to help shape these important policies and practices.

[signed]

---

7 November 2002

[redacted]  
Vice-President for NetDiscovery Strategy

21355 Ridgetop Circle  
Dulles VA 20166

s.19(1)

tel: +1 703.948.4305

mailto: [redacted]



Cloutier, Marie

s.19(1)

From: [REDACTED]  
Sent: 2002 Nov 11 1:20 PM  
To: la-al@justice.gc.ca  
Subject: Government of Canada to Review Lawful Access Laws

As a scanner user (a legitimate hobby) I have difficulty with both the proposed legislation and extant legislation which makes or proposes to make my hobby either illegal or less legal than it currently is.

Scanner users help keep the police forces of this country honest and above board. They help prevent abuses of the various freedoms currently guaranteed by the Charter of Rights and help prevent misuse of technology by the various police forces in action in Canada. However, both extant and proposed legislation in some aspects makes the hobby difficult.

One example is the requirement that Digital Scanners be licensed. This regulation has existed since the mid-1990s based on a statement made by the minister at the time, and at the time it was put in place it may well have made sense, since there were few, if any, uses of digital technology in the communication of scanable traffic. Now technology has changed and almost every device will soon be digital, so that analogue radio communications will cease to exist.

However the requirement that digital scanners be licensed continues to exist in Industry Canada internal procedures (IPC2104 from November 1996) and Industry Canada seems to be taking the position that they will NOT issue a license to the average Canadian citizen... To require someone to first become a holder of an amateur radio operators license is ridiculous, since the user of a scanner as a hobby is NOT interested in transmitting anything and therefore does not need to know about 50-70% of what is on the test for that license.

Further, all this will do is encourage Scannerists to bring the digital scanners or analogue scanners capable of digital scanning in from the US or other locations where they are legal, to the detriment of Government revenues, since they will have to be brought into Canada without being declared and therefore GST and PST will NOT be paid. A regulation that CANNOT be enforced (scanners do NOT broadcast and therefore are virtually impossible to detect) is a pointless regulation. It can only serve AFTER the fact to make a person with a legitimate hobby into a criminal.

It will NOT stop a terrorist or criminal gang - if they know about scanners they will have them from outside Canada, with all the bells and whistles. All the law will do is make it harder for the legitimate, above board, hobbyist or retired person to enjoy their hobby and link to the world. IS this intended?

Therefore I suggest that:

1. The license requirement for digital scanners (handheld or desktop) such as the Uniden BC250D be changed to match the license requirement for the Uniden BC245XLT, which is the SAME scanner without the ability to accept a small add-on card that permits the newer analog scanner to become a digital scanner.
2. Any restrictions on the hobby of scanning be carefully thought out to preserve privacy for those who truly deserve privacy and NOT create a privacy right where none is deserved (for example standard police communications do NOT deserve privacy rights any more tomorrow than they had yesterday).
3. Permit encryption where it is needed - for example cell phone communications, and NOT where it is not needed - fire calls, standard police calls, etc.
4. Require police to get a court order to permit them to use encryption and secure communications when investigating crimes, terrorism, etc. on

a case by case basis, similar to their need for a search warrant. The point is identical in nature and protects the average Canadian from the creation of a secret police state.

I am certain that the police will dispute my position on what is and is not subject to privacy rules, but the police work for the citizens of Canada and we should have the ability to monitor what they do normally.

There MAY well be occasions where encryption and privacy protection is needed by the police in an investigation, but then they should need to convince a judge and get a court order to permit them to hide their activities, just as they need to get a court order to do a search in someone's home, etc. Police are NOT and should not be automatically entitled to act and hide their actions, even if they think they are or should be.

s.19(1)

North York, ON, Canada

**Cloutier, Marie**

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Nov 14 9:31 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Proposal re Internet Providers and surveillance

Dear Sirs,

Proposal re Internet Providers and surveillance

I am opposed to simplification of Internet surveillance.

I came to Canada in 1957 from the Netherlands, partially to find more freedom in this country than was available in Holland. The tight control on everything under the sun, from a work permits, permits to move and permits to build your own home with your own money was a far cry from the liberty I found in Canada, where for elections a house to house survey had to be conducted to establish the voters list.

Slowly this liberty which I so appreciated has been eroded. The Canada Pension Plan was effectively made **COMPULSORY**, also for Canadians with adequate pension provisions. The SIN number was **PROMISED** to be limited for social provisions, but made **COMPULSORY** for income tax purposes and became a **CONDITION OF EMPLOYMENT**.

No Interconnection of data-bases was **PROMISED**, but nevertheless interconnected in Human Resources. Also under the Income Tax data-bases are interconnected to "update" the voters list. The op-out provision is violated in the polling station where only attentive persistence prevents being listed on the list by the default on the form.

The introduction of an identity card for every Canadian is under serious consideration today. No doubt that will be interconnected with the data-base for internet users.

From my own experience as manager of people in telecommunications I know that any information which is readily accessible will be used and misused, notwithstanding "safeguards" and "protections". The only way to guard private information is to have it **NOT AVAILABLE**.

The Netherlands and the European Union have moved "forward" (back really backward) and will - no doubt - demand Canada to follow their schemes of total control over every person.

Let us keep Canada free, or did I come in vain?

[REDACTED] Edmonton

Cloutier, Marie

s.19(1)

From: [REDACTED]  
Sent: 2002 Nov 14 9:41 PM  
To: la-al@justice.gc.ca  
Subject: Lawful Access

To whom it may concern:

As a Canadian citizen, born and raised, who relies on the Internet for both work and pleasure, the topic of lawful access is very important to me.

As the Internet becomes more and more invasive, the user base who pays for these services need to be protected in every way possible. It is far too easy to overlook the best interests of the majority, in order to meet a mandate of government.

While it is very important for law enforcement to be able to track down and arrest criminals, and while it is very important for them to have the tools to do so, using blanket security measures only causes problems and hassles for the law-abiding citizens, most of whom, unfortunately, will go along with whatever our Government puts into law, if not merely out of ignorance of the true repercussions of any law or act.

We've seen the negativity of blanket security measures at the border between Canada and the United States. In the instance of American border officers fingerprinting Canadians born in certain Middle Eastern countries, the greater issue at stake was what the Government did about it. Unfortunately for Canadians, it was the press who was able to take most of the credit, for making this ridiculous mandate public. Yes, the Foreign Minister was in contact with U.S. officials, and yes, the U.S. has officially backed down on their hard line stance, but the fact that the U.S. is constantly pressuring Canada to join, on the front line, their so-put "War on Terrorism," means that there is also pressure for Canada to enact stricter laws on security, including lawful access. Needless to say, this means that it's up to the Government of Canada to do for Canadians what the United States claims to be doing for their citizens: Looking out for the best interests.

This lawful access consultation is a chance for our Government to take the world lead in keeping the interest of its citizens at heart, and to show the world that, in the face of terrorism, we can truly fight to maintain the freedom, and anonymity, of Canadians.

The issues I personally have with this consultation are these:

1. What, exactly, would be allowed to be gathered, when, why, and how?
2. How will law enforcement be held accountable to the information they want to gather, and what law will be enacted to prevent abuse of the lawful access policies by service providers and law enforcement?
3. How will I, as an access consumer, know that when I am connected to my service provider, my privacy and anonymity are being respected?

First, the access guidelines. It should only be lawful to gather information when there is an order to do so from the law. Put more simply, it should be illegal for access providers to gather any more information than is necessary for operation. For example, if there is no reason to warrant my personal e-mail, my access provider should not be allowed to store or read my e-mail. On the other hand, if there is more than suspicion of my participation in illegal activities, and there would be no problem with law enforcement gathering other information about me, then the access provider would "turn on" the surveillance equipment, store the information, and turn it over to the authorities. Making sure that it is illegal to collect for no reason, as the law states now for what it does cover, will help to ensure the security of Canadians.

Second, what law or committee is going to be put in place to ensure that law enforcement collect only what they are allowed to, and only what they need

for their purpose? Example: if my e-mail is needed, but not the history of what websites I've visited, it should then be illegal for law enforcement to obtain a record of my web history. Therefore, there needs to be a system of checks and balances to ensure that access providers and law enforcement are only collecting what they need. Again, this avoids the blanket measures that, because of the sheer quantity of information, would even slow down the law enforcement process.

Third, the issue of privacy. In the U.S. and in the U.K., general privacy and anonymity are being eroded in the name of "security." On the Internet, it's unnerving enough to think that every click of my mouse is being logged, simply for statistics, without having to think that, on top of that, the information is being saved and could be used against me. What law will be put in place to ensure that my online privacy is secured? This not only applies to lawful access by law enforcement, but all Canadians should feel safe in their day to day lives. When we talk on the phone, we know that we're not being tapped by the Government (I hope). When we "surf the 'net," the same sense of security should apply.

To sum, lawful access to the private information of criminals should be a fundamental of law enforcement. Lawful access to the private information of the rest of us should be greatly limited. These lawful access laws need to be written, not with service providers, or even law enforcement, but with the end users in mind. The 73 year old grandmother in Victoria has no thought of breaking the law. She only wants to see the pictures of her grandkids. The 13 year old in Montréal only wants to keep in touch with his friends. Why should their online activity be monitored? It shouldn't, and, in the process of hunting down and punishing criminals, the rights of the average Canadian should be held at the forefront. Even in front of the law enforcement, or other countries who desire that Canada bow to a threat we didn't create, and have no power to control. If we, as a country take a stand in the face of this mindless pull to "security," the world will have no excuse but to take note, once again, of how great this country really is. On the other hand, if we bow to international pressure, if we don't hold our own, if we're not taking our best interests at heart in the face of this international scramble, then we are no longer our own nation under the Commonwealth, we are nothing more than a puppet on the international stage, waiting for the next puppet master to make us bow to them.

Respectfully,

s.19(1)



## *Regina Police Service*

*Dedicated To Building A Safe & Caring Community*

Your File \_\_\_\_\_

Our File \_\_\_\_\_

November 14, 2002

Lawful Access Consultation,  
Criminal Law Policy Section,  
5<sup>th</sup> Floor,  
284 Wellington Street,  
Ottawa, Ontario.  
K1A 0H8

Dear Sir/Madam:

Attached is a paper prepared by Cpl. Mark Kelsch from our  
Intelligence Unit. Please accept this as a response to the Lawful  
Access Consultation document.

Yours truly,

s.19(1)

Deputy Chief of Police.



## **Lawful Access Consultation Document**

### **Legislative proposals**

-This document proposes that all service providers be required to ensure their systems have the technical capability to provide lawful access to law enforcement.

### **Introduction**

We are fortunate in Sask because the main "telco" service provider is of course Sask Tel. They do the maintenance on all the landlines in the province, and other providers like Telus rent from Sask Tel. All the switching still goes through Sask Tel, so as a result we as a Police Service have the ability to intercept through their switching stations to our office.

In other larger centres, such as Toronto, telephone companies run their own lines and use different kinds of electronic switching that is not compatible with the technology used by law enforcement. The systems that the telephone companies develop are designed to provide customer service to the paying public, and not service the policing need to intercept the communications.

When police services ask for "assistance" as the criminal code suggests, the phone companies say sure, but who will pay for the technology, or if the technology exists how much should they charge for it.

### **Regulations**

Question is what regulations should be in place to ensure Telco's:

- have the equipment in place to intercept private communications.
- how many lines should they be capable of intercepting?
- ensure people at the Telco are not security risks to the project.
- ensure the Telco people are competent, reliable and are deployed in a timely manner.
- should these regulations provide fee schedules for the services?

If there are some regulations imposed, the interests of the Telco's must be considered. In Saskatchewan, at least for now, there is adequate equipment to intercept as much and as often as we need. We always use secure people to set up the switching in Sask Tel and have developed good working relationships, and we do pay for the services. We get more service than we pay for in that Sask Tel Security will bend over backwards to help and will even come out to the RPS building to help with equipment often without costs.

If there is not a fee schedule with "reasonable" costs attached to certain services, then the quality of the service will fall. If for example, the fee is too small or does not exist, when we ask for something we get it tomorrow or next week when it is really needed today.

## **Orders to provide subscriber information**

### **Issues to be considered**

-should there be a specific production order in relation to customer name and address, who should have access to this, what data should the service provider collect, and should this obligation be extended if they are not currently collecting the information on their customers now?

The trouble for us is when you are planning to do a project, or researching to see if there is even a telephone line to go up on, you need to make inquiries with the service provider. If there are several service providers, of course you need to check with each one. If we inquire with Sask Tel and say we may be working toward a DNR or wiretap authorization they will usually provide unpublished information. They do record the Police members name etc. in case of a complaint so they know who made the inquiry and the reason for it. This covers them from civil problems and keeps the police from abusing this since your name is attached to the inquiry for the information.

Some data that is helpful is name, address, where the phone is hooked up at, who the reference is, and other credit information such as the subject's work place.

If you are not opposed to it, your name and number are published and are available to the general public. Personal information such as your work place, references, etc. are not something you would expect Sask Tel to give out, meaning you have some expectation of privacy. The issue is, if the police needs this information, how hard should it be for them to get this information? In larger centres with many telephone providers I know they need a warrant to get the information, and this will be the case as time goes on in Saskatchewan. This seems like a lot of work for the information you get in return and it would assist law enforcement to have orders to obtain this subscriber information that are simplified.

## **Assistance orders**

We currently craft paragraphs within search warrants, tracking warrants, and Part Six Affidavits and others that ask for assistance from outside agencies like Sask Power, Sask Tel, apartment managers, service station owners etc.

These paragraphs are tailored to the particular project. For example, if you are searching an apartment or installing a room probe, it may be of value to ask the assistance of the building manager to open the apartment door. The paragraphs we include can be innovative, and as long as they are not illegal or unconstitutional and the justice or judge signs off giving you "Judicial Authority" then you can proceed to ask for assistance.

The question, "Should assistance orders spell out more clearly the scope of what a person may be required to do to give effect to the warrant or authorization?" is difficult to answer since the requests for assistance are made in general terms. This is because investigators want to cover all bases, and if they are real specific and some part of the plan changes then the specific request may not apply. On the other hand, it is abusive to ask "For anyone, anywhere to help with anything" so it must be balanced and reasonable.



## **Interception of Email**

If a law enforcement agencies is wanting to intercept real time Email transmissions, they should be requires to obtain a Part XI authorization and the interception would best be attainable by intercepting the communication at the Internet Service Provider but should not be restricted to that area, depending on the investigational needs ( If a Canadian Police agency wanted to intercept Emails sent from Nigeria and were funnelled through a ISP in Denmark and was sent to Canadian victims, the easiest and most likely retrieval point would be the victims computer in Canada)

### **Customer Name and Address (CNA)/ Local Service Provider Identification (LSPID)**

I think a system that retains the CAN and LSPID information would be a valuable asset to law enforcement and security agencies, but I think its implementation would be very difficult as there are presently systems and programs specifically designed to cloak the identity of Email and Internet users. If such a system or retention of this information was requested by law then the Service providers should have to comply of face sanctions from the CRTC or penalty under the Criminal Code of Canada, in some worse case scenarios the International Courts in the Hague may have to be empowered to order or stop some ISP from operating worldwide.

**Cloutier, Marie**

s.19(1)

**From:** [REDACTED]  
**Sent:** 2002 Nov 15 3:43 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Lawful Access Consultation

November 15, 2002

This matter has just been referred for my review and unfortunately I will be away until December 2nd. I may be able to provide comment while I am away but failing that would a submission in early December be ok?

[REDACTED]  
Legal Services  
Department of Justice (NS)  
4th Floor - 5151 Terminal Road  
P.O. Box 7  
Halifax, NS B3J 2L6

Ph: (902)424-8567  
Fax: (902)424-7120

email: [REDACTED]

This message and accompanying attachments contain confidential or privileged information that is intended only for the use of the individual or entity to whom it is addressed. Any dissemination, copying or action taken in reliance on the contents of this communication by anyone other than the intended recipient is strictly prohibited.

If you received this communication in error, please notify me immediately at the above e-mail address and delete the e-mail. Thank you.

**Cloutier, Marie**

---

**From:** [REDACTED]  
**Sent:** 2002 Nov 15 10:37 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Electronic communications access

s.19(1)

It seems to me that, at its core, this is simply yet another surveillance initiative, such as we have seen an increasing number of since 11 September 2001.

Like most such initiatives, it'll make everyone feel watched, and perhaps result in a few people being caught for otherwise insignificant minor offences, at the cost of everyone's privacy.

Real criminals/terrorists (and soon, all privacy-wary people!) will be using public-key encryption, which they surely do already.

What we're really leading to is, underneath all the fancy wording, a capacity to compile lists of people who visit "objectionable" web sites, make/receive phone calls to "suspicious" persons, and so on. All in all, the kind of generalised surveillance, based on the premise that everyone is suspect, which shouldn't be going on in a free society.

**Cloutier, Marie**

---

**From:** [REDACTED] s,19(1)

**Sent:** 2002 Nov 15 1:37 PM

**To:** la-al@justice.gc.ca

**Subject:** Lawful Access Response

Hi:

Please find attached the position of the Canadian Information Processing Society on Lawful Access.



CIPS, 2800 Skymark Ave, Suite 402, Mississauga, ON, L4W 5A6  
(905) 602-1370 phone and (905) 602-7884 fax  
[www.cips.ca](http://www.cips.ca)

*Providing the only professional IT designation in Canada.*



Deliver By E-Mail: [la-al@justice.gc.ca](mailto:la-al@justice.gc.ca)

November 15, 2002

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington Street  
Ottawa, Ontario, K1A 0H8

**Subject: Consultation on Lawful Access**

Thank you for the opportunity to comment on the proposals to provide for capability to law enforcement agencies to intercept communications and to provide for search and seizure of information pursuant to legal authority.

With approximately 8500 members, CIPS is Canada's largest association of IT professionals, representing the interests of IT professionals to industry and government. Through the volunteer efforts of its members, CIPS is involved in a number of initiatives relating to public policy, setting standards within the IT profession and providing assistance to its community. Our advocacy role is intended to reflect the public interest as well as that of our members.

#### **Preamble**

Privacy is a right upon which many other democratic rights are founded. For example, the ability to participate in private political discourse without fear of surveillance by the state is founded in part in the privacy rights of the individual. As a result, privacy is a cherished value among Canadians. This attitude of Canadians has been validated by many surveys over the past decade.

At the same time, CIPS recognizes that privacy is not an absolute right. The privacy rights of individuals must be tempered with the reasonable information requirements of the state (eg., census information).

Law enforcement activities (including related justice activities) are, for the most part, hostile to the individual's privacy interests. When a crime is committed, or thought to have been committed, activities are initiated that result in individuals coming under a great deal of scrutiny. We are not only talking about the privacy rights of those charged or convicted. Depending on the nature of the crime, the victim, friends and family members and others thought possibly to be perpetrators are also investigated.

Finally, the court system is open to the public and, with few restrictions, is reported upon by the press.

Notwithstanding the intrusive nature of the law enforcement and justice system, the Canadian law enforcement system is a reasonable, and sometimes a necessary, intrusion into the lives of Canadians with the result that a Canadian society, as we know it, is maintained.

Notwithstanding the justifiable intrusiveness of the justice system, the proposed powers for law enforcement agencies must be subject to civilian and judicial oversight.

### Summary

Against this backdrop of genuine needs of law enforcement and the scepticism of the Canadian public, CIPS will present a number of concerns and propose a number of counter-balancing measures to mitigate the concerns.

We use the term "counter-balance" here to suggest that Canadians should not relinquish privacy in response to the needs of law enforcement. Rather, we will propose that there should be counter-balancing proposals, such as civilian over-sight and criminal offences, to ensure that the proposed powers are deployed only where justified, and in a manner that is consistent with the law.

CIPS will raise concerns or make suggestions with respect to:

- definitions for law enforcement and service provider.
- concern that the proposals can be easily circumvented by those under surveillance by using encryption technology
- concerns about disclosure of investigatory materials to law enforcement agencies in other countries
- concern that a Cabinet Minister does not represent citizen's interests during the Regulation-making process.
- concern about who might have access to investigatory materials after they are collected
- commentary that the investigatory material might be presumed to contain personal information and be subject to access under the *Personal Information Protection and Electronic Documents Act*
- concern about the proposal to establish a subscriber database, and
- identification of additional areas of concern with respect to illegal devices and the need to exercise caution so that innocent distribution of a virus is not criminalized, nor is possession for legitimate research purposes.

CIPS will also suggest that there should be a number of new offences with respect to the secondary use and disclosure of the investigatory materials.

### The Lawful Access Consultation

As a general observation, we find the consultation document lacks justification for the proposed lawful access measures and lacks specific problem statements that need to be addressed, nor does it contain reasonable counter-balancing measures to protect the public interests and to prevent misuse of the proposed powers.

Admittedly, CIPS members for the most part, are not lawyers. But litigants seem to have the ability to seize electronic records where necessary. As a result, CIPS questions why law enforcement agencies believe the current tools to be inadequate.

Notwithstanding the general concerns of CIPS, we believe that it would be unreasonable not to provide some additional tools to law enforcement agencies to ensure that investigations are not unreasonably hindered by virtue of the fact that the medium is the online world. We also believe that some parts of the proposal cannot be dismissed without further analysis. Therefore we provide more detailed comment below.

CIPS would take a very different stand on the issue of lawful access if it were not for the requirement for the law enforcement agency to obtain a Court order to produce the records. Any attempt to weaken this safeguard would be viewed by CIPS as contrary to the "public good".

### **Investigatory Materials**

In this response, we use the term "investigatory materials" to describe electronic communications that are intercepted, stored and disclosed to a law enforcement agency under the authority of a search warrant, Order to Produce, or other legal instrument.

### **Definition of Law Enforcement**

The definition of "peace officer" under the Criminal Code is sufficiently broad that it includes many officers that are better characterized as compliance officers. Indeed the definition of "peace officer" includes the mayor of a community. Many provincial statutes confer "peace officer" status on compliance officers. Our view is that the proposed powers should be restricted to municipal, provincial and national police officers and bona fide investigators of national security agencies.

Furthermore law enforcement agencies that might take advantage of the proposed powers are not defined. There are many Canadian law enforcement agencies that might be better characterized as compliance agencies. Even where these compliance agencies have the power to lay charges or make arrests, the proposed powers should be restricted unless the compliance agency has turned the investigation over to a municipal, provincial or national police force, and there is conspiracy involved or electronic communications are fundamental to the commission of the crime.

Finally, not all investigations undertaken by police officers are law enforcement investigations. Police officers will sometimes conduct investigations of other police officers in their role as an employer (eg., preparation for a grievance or worker's compensation hearing). Orders to produce should not be available under these circumstances.

### **Definition of Service Provider**

The consultation paper refers to the problem, from a law enforcement perspective, posed by the multitude of service providers and the need to have some sort of central registry to allow law enforcement agencies to efficiently identify which service providers should be served with an Order to Produce should one of their subscribers come under surveillance.

The proponents of this proposal seem to have greatly underestimated the magnitude of the problem by apparently overlooking at least two potential groups of service providers. Arguably, every employer and other organization that provides their own telecommunications (voice over IP) and Internet services will be required to provide intercept capability and to register and update the registry with subscriber information. Indeed the federal government is a very good example of this with hundreds of thousands of e-mail accounts and connections directly to the Internet. In this example, should a federal employee come under surveillance under these provisions, their employee accounts might also come under surveillance.

Another group of potential service providers are those that operate discussion groups on private web sites and virtual communities where people with like interests share ideas. The public can register for these virtual communities without authentication making it virtually impossible for those service providers to register their subscribers in a national database.

The end result appears to be a patchwork of coverage.

### **Rapidly Evolving Environment**

While the consultation paper alludes to technological developments that affect lawful access, the consultation does not provide any assessment of the nature or scope of the problem, the effectiveness of the proposals, and whether there are options that might be considered to mitigate the problem.

To underscore this concern that the proposals do not address specific problems, many wrongdoers are smart enough to use encryption and defeat the intent of the proposed surveillance. CIPS is not suggesting that possession of encryption technology should be illegal, or that developers should provide a "back door" for law enforcement. But we are suggesting that the proposed measures can be easily circumvented.

Of even greater concern is the statement on page 4 that "the global nature of these technologies can create significant jurisdictional problems in criminal and terrorist investigations". This comment presupposes that there must be sharing of information with other countries. CIPS recognizes that mutual assistance treaties are in place between Canada and other countries. However, this document does not discuss the controls and over-sight mechanisms that are, or should be, in place to ensure that sharing of information is reasonable. Increasingly, the U.S. is demonstrating an unreasonable position on the issue of trans-border flow of Canadian residents. This is evident by the travel advisories that have been issued by the Government of Canada.

There is no reason to believe that the U.S. government will temper their demands for information about persons under investigation for serious, as well as, minor offences. As a result, we believe that there should be limited sharing of information extra-territorially. CIPS proposes that before initiating any surveillance where the investigatory materials are likely to be shared extra-territorially, the search warrant, subpoena or other legal instrument authorizing the activity must be approved by a superior court judge.

### **Requirement to Ensure Intercept Capability**

Regulation is a method of implementing law that does not undergo the same level of scrutiny as that of a statute.

While CIPS does recognize that Regulations are an appropriate mechanism to implement technical standards, we also believe that the process as described on page 8 is biased in favour of industry concerns (as represented by Industry Canada) and law enforcement (as represented by the Solicitor General). As the Solicitor General cannot effectively represent the interests of both citizens and law enforcement at the same time, no one at the Cabinet table will advocate on behalf of citizens in the process of making Regulations. We consider this to be a serious deficiency in the proposal.



On the issue of reimbursement of the service provider, many organizations are called upon to monitor and report certain types of activities (eg., financial institutions are called upon to report certain types of financial activities, and all organizations are required to produce records when required to do so by Court order) without reimbursement. The proposal requires more of the service provider than monitoring or reporting, but the requirement to participate with law enforcement agencies is a civic duty and should not be reimbursable. In the absence of any argument that the communications service providers are faced with an unjustified financial burden, this appears to be a cost that should be borne by industry. Policy makers must also be mindful of the effect that the above discussion on the definition of service provider might have on the proposal.

### **Access to Investigatory Materials**

The lawful access proposals referred to in the consultation are predicated on the assumption that the information needs of the state sometimes must take precedence over the competing privacy rights of individuals. But there are other facets of privacy that need to be considered.

Privacy is predicated on the notion that personal information should not be used for purposes other than those for which the information was collected. It is apparent to CIPS that various parties may seek access to the information collected by the service provider for reasons other than the original purpose.

**Presumption That Record Contains Personal Information.** Where an individual is under surveillance for activities that are unrelated to employment (eg., laundering of personal funds), it is our view that the records should be presumed to contain personal information of the person under investigation and must be protected.

If one accepts the position that the investigatory materials contain personal information, one must also accept that these records are highly sensitive because of the context in which they are collected. Records that are collected as part of an investigation into a possible violation of law are considered to be particularly sensitive by virtually all privacy laws.

Public policy makers must also consider that not all of those under surveillance are actually involved in wrongdoing. For example, innocent parties may be put under surveillance solely because of their relationship to the suspected individual. Or troubled teenagers may be involved in proliferation of viruses and therefore be justifiably under surveillance. But their communications may also communicate on a variety of other topics that affect troubled teens including suicide, sexual activity and disease. It would be an unjustified invasion of privacy if the investigatory materials were subsequently used for unrelated secondary purposes (such as victim impeachment during a sexual assault trial or for job applicant screening).

In other circumstances, the communications under surveillance may be subject to solicitor-client or some medical privilege. These records should be segregated and access should not be provided unless first screened by a judge.

For these reasons, secondary access and use of the information provides a significant privacy threat to those under surveillance. We propose the following information access schema.

**Law Enforcement.** The law enforcement agency obtaining the order to produce, or other instrument which requires the service provider to collect and disclose the personal information should have access consistent with the provisions of the Order.

**Service Provider.** The service provider has no right of access to the investigative materials except as provided in the Order to Produce. Normally, this access should be restricted to that access which is required to assist the law enforcement agency.

**Person Under Surveillance.** The person under surveillance should have access to the investigatory materials under the *Personal Information Protection and Electronic Documents Act* (PIPEDA) after the surveillance has been completed and the person is advised of the surveillance. This right of access may be restricted by the Order to Produce. This is unlikely to interfere with a law enforcement investigation because the individual will have received a copy of the investigative materials (eg., e-mail messages) in the course of going about their day-to-day activities. However this right of access will allow the individual to review the surveilled communications from the perspective of the law enforcement investigation.

This requirement suggests that once a service provider is required to collect and store communications in accordance with an Order to Produce, the service provider or the law enforcement agency is required to securely maintain that collection for a period of time that is long enough for the individual to seek access to their personal information. Many privacy laws consider the minimum retention period for personal information to be one year after last use.

**Employer.** Employers may seek access to the investigative materials particularly where the employer has provided the communications equipment or service. Where the individual is investigated for activities unrelated to employment, consideration should be given with respect to employer right of access. Increasingly, some countries have restricted employer's right of access to employee e-mail in favour of employee privacy. For example, the *Regulation of Investigatory Powers Act 2000* in the United Kingdom only allows monitoring of e-mail where there are reasonable grounds to believe that both the sender and recipient have consented to the monitoring.

**Third Parties.** Various third party (private investigators, lawyers, insurance companies, etc.) interests could be advanced by access to the investigatory materials. While it is reasonable for the state to seek access to records involving wrongdoing, it must be remembered that the surveillance will capture communications on a wide range of other topics. So that individuals are not pressured into consenting to the third party access, it should be an offence for a third party to request consent for access to investigatory records.

#### **Other Mechanisms to Provide Subscriber and Service Provider Information**

CIPS recognizes that it is not an easy task for law enforcement to determine the local service provider identification (LSPID) information. Nonetheless, CIPS believes that a subscriber database is an unwarranted intrusion into a person's private realms. Individuals have a right to be anonymous, insofar as it is possible, on the Internet. There are bona fide reasons for this ranging from privacy (eg., a person living in a small resource-based community might want to keep contributions to an environmental group private), to reduction in profiling activities. At one point, industry sought support for information on the outside of the e-mail "envelope" to be public and not subject to privacy laws. This suggests that they would welcome the opportunity to provide for matching of all *persona* that an individual might possess.

CIPS does not accept the recent CRTC approval of conditions under which Bell Canada could release LSPID information. The CRTC approval does not necessarily represent a broad consensus of Canadians on this issue.

CIPS previously noted (in the section on Definition of Service Provider) the significant problem of identifying who is covered by this proposal (eg., does it apply to employers and to virtual communities). You will recall that the service providers for virtual communities do not require authentication of a subscriber before providing services. Unless their business model is changed, the national registry will be a patchwork at best.

The notion of a national registry is predicated upon the notion that law enforcement must be able to accurately identify their targets in that database. That would suggest that service providers would have to collect and report more than a name and address and subscriber identifier. It is our view that the Canadian public will find the collection of a national identification number (such as the social insurance number or a new national identifier) to be unacceptable.

In the final analysis, CIPS believes that the public has a right to anonymity on the Internet (insofar as that is possible) much the same as the public can use cash for anonymous transactions in the real world. There is nothing sinister about this and it is repugnant to force citizens to register before undertaking lawful activities.

### **Compliance Mechanisms and Counter-Balancing Proposals**

**Scope of Proposed Powers.** The proposed powers should be available only to police officers and intelligence officers who are investigating serious crimes such as organized crime, money laundering and terrorism where there is evidence that electronic communications are being used to conduct criminal activity. The powers should not be available for "fishing expeditions" nor should they be available for relatively minor offences.

**Civilian Oversight.** CIPS believes that approval of legal instruments by a justice of the peace is not a sufficient safeguard. At a minimum, the "legal instrument" providing access should be an order of a Superior Court. We also propose that orders to produce and other legal instruments should be subject to civilian oversight. We have not provided details how this might work but it should likely be a retroactive oversight mechanism by a special committee that reports to Parliament.

As already mentioned, there should be a senior Minister to represent the interests of citizens in the regulation making process and civilian over-sight.

**Audit Trails.** Audit trails should be required for all access to the investigatory materials by law enforcement, services provider and third parties.

**Safeguards to be Provided by Service Provider.** To prevent unauthorized access to the investigatory materials while stored at the service provider's site, the investigatory materials should be encrypted with access only provided to authorized individuals. An audit trail of all activities should be produced.

**Offences.** To protect the public from potential abuse and misuse of the investigatory materials, CIPS proposes that a number of new offences should be created. These offences should apply

equally to law enforcement agencies and to businesses (eg., private investigators and insurance companies to name two), organizations and the public.

CIPS proposes that the following should be offences:

- Seeking access (eg., simply asking for access) to electronic communications without an Order to Produce or similar legal instrument.
- Collecting electronic communications without a legal instrument allowing the organization to do so.
- Disclosing electronic communications collected under the authority of a legal instrument, to any person not explicitly provided access in the legal instrument.
- Accessing, or attempting to access, investigatory materials under false pretences.

Penalties should be similar to those under the *Personal Information Protection and Electronic Documents Act*. In serious breaches of confidentiality and the above-noted offences (eg., those involving health or law enforcement information, or undertaken with a view to discredit an individual for small "p" political purposes), the penalties should include the potential for incarceration.

**Employee Rights.** Where an employer (as a "service provider") might be served with an Order to Produce records of an employee, the employers should be prohibited from disciplining the employee solely on that basis.

### **Illegal Devices**

The consultation suggests that there should be new offences in relation to illegal devices such as viruses. CIPS believes that viruses and similar devices do need controls and offences do not seem unreasonable. But we do suggest that care must be taken not to prohibit the legitimate activities of *bona fide* researchers and companies that possess these devices for analytical purposes and to develop safeguards (eg., create signature files so that the viruses can be detected and destroyed).

Nor should a person be guilty of an offence if they have an undetected virus or other device residing on their computer that is transmitted without their knowledge.

An area of illegal devices that may need additional attention is "spyware". These products collect information about a computer user's browsing habits (known in the industry as "click-stream" data) and surreptitiously transmit it to an information broker. Some browsers and media products reportedly have this capability. The software end user license agreement (EULA) refers to this practice, however, the surveillance is surreptitious and, in our view, unethical. The practice poses certain legal issues with respect to one person consenting to surveillance (if he or she is aware of it at all) on behalf of all users of that computer, or where the person accepting the terms of the EULA is a minor. For these reasons, we believe that these products should be banned from manufacture, sale or distribution (eg., preloaded on computers) in Canada.

Unethical and fraudulent businesses are engaged in mass mailing (millions) of unsolicited e-mail for commercial and other purposes (SPAM). This activity results in lost productivity and increased salary costs while employees process these messages. It also increases costs to the organization to deploy increased storage capacity. Our view is that this activity should be a Criminal Code offence. Care should be taken to ensure that legitimate businesses that send

unsolicited e-mail to others that reasonably have, or ought to have, an interest in the product or service are not in contravention of the law.

Related to the issue of SPAM is the activity of those who misrepresent themselves. One way this is done is to use someone else's e-mail address in the "reply to" line of an e-mail. Our view is that this constitutes theft of identity and it damages the reputation of the person whose identity has been usurped. In extreme cases, it may result in the innocent party's e-mail and Internet services being terminated. Our view is that misrepresenting one's self as the sender of an e-mail for unauthorized purposes should be a criminal offence that is similar to fraud. Care should be taken not to criminalize providing bogus information where the intent is to protect one's privacy.

### **Interception of e-Mail**

The consultation paper suggests some ambiguity in law with respect to a reasonable expectation of privacy. CIPS believes that e-mail should be afforded the same privacy protection as regular mail and telephone conversations. It is our view that it should be an offence to intercept or otherwise access e-mail at any point during the transmission between the sender and recipient unless the access is authorized by a search warrant or subpoena or other legal instrument.

### **Summary**

In closing, CIPS members have a tremendous respect for the job done by the law enforcement community. But at the same time, we believe that the proposals in their current form will not work. More importantly however, we believe that the proposals do not contain reasonable safeguards to counter-balance the powers of the state and, as a result, are unwarranted in their current form.

We hope that this letter provides constructive input in the dialogue.

Sincerely,

CANADIAN INFORMATION PROCESSING SOCIETY



President

s.19(1)



s.19(1)

Executive Vice President  
Corporate Affairs & General Counsel



8<sup>th</sup> Floor  
555 Robson Street  
Vancouver, British Columbia  
Canada V6B 3K9

604 697-8020 Telephone  
604 437-8560 Facsimile

November 18, 2002

Morris Rosenberg  
Deputy Minister  
Justice Canada  
284 Wellington Street  
Ottawa, Ontario K1A 0H8

Dear Mr. Rosenberg

On August 25, 2002, Justice Canada released a paper entitled Lawful Access – Consultation Document, soliciting public comment on proposals to better enable law enforcement and security agencies to conduct investigations. I wrote to Mr. Richard Mosley asking for an extension to the filing deadline so that comprehensive input could be prepared on this important topic. I also understand that, in early September, a number of associations also wrote to request an extension to the period allotted for the submission of comments. These included:

- Canadian Cable Television Association,
- Canadian Association of Internet Providers
- Canadian Wireless Telecom Association
- Canadian Advanced Technology Association
- Information Technology Association of Canada

I am pleased to see that Justice Canada has granted an extension to the consultation period to December 15, 2002. The additional time to consider the implications of the proposed changes is appreciated and I want to thank you for this consideration. Nevertheless, the topics raised in this consultation require a review that is an extremely complex undertaking. TELUS finds it difficult to comment on the proposals set out in this Discussion Paper without having an appreciation for the entire operational framework. We have attended several consultation meetings with officials from the various Departments and Agencies involved, and several matters are still unclear to us.

The proposed legislation will impact several acts of Parliament, including the Criminal Code, the Radiocommunication Act, the Competition Act and PIPEDA. The ensuing implementation by law enforcement staff at three levels of government (federal, provincial and local) will require clarity with respect to the regulations, and perhaps the working guidelines, if the intent of the legislation is to be effectively realized with the least disruption to existing networks. To illustrate one area of concern, our current understanding is that small ISPs, hotels and universities might be exempted from complying with the obligation to provide intercept capabilities. Beyond the simple fact that this would leave many holes in the intercept net, it would also change the competitive environment by making one of our telecom

services, Centrex, a less attractive option for such users than providing their own local PBX equipment, because the latter would be exempt from lawful access requirements.

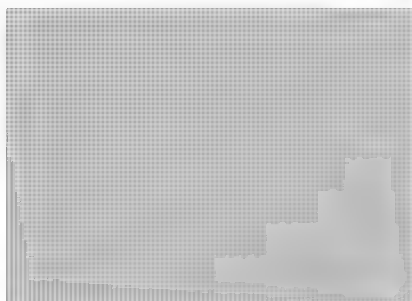
A second emerging concern relates to the growing issue of reimbursement for our operational costs relating to law enforcement's requests for lawful access services. While CSIS, the RCMP and a number of other provincial and municipal police forces have, in past, acknowledged these operational costs and have willingly paid for them, two local police forces have not. Now that the lawful access services requested will be more comprehensive in nature and arguably more costly to provide, this matter needs to be addressed.

TELUS finds it difficult to fully ascertain all of the various impacts that the proposed legislation will have on our industry. Despite our best efforts, we are still unable to see how all the pieces of the Lawful Access legislation, which will govern our relationship with law enforcement into the future, are going to come together to form an effective interception regime.

Therefore, TELUS proposes that the Department release a draft bill and the anticipated supporting regulations so as to allow for a fulsome dialogue between industry and government. Frankly, TELUS is uncomfortable providing comments on the current public discussion paper that outlines, only in very general terms, requirements that could have a dramatic effect upon the entire communications sector. The privacy, technical, operational and service issues arising from implementation of the paper's proposals may have a major impact upon TELUS and the industry as a whole. These issues deserve a comprehensive and thoughtful review with a full understanding of the draft legislation and regulations. While I acknowledge that a release of the material for public comment, as proposed, might extend the consultation process, I believe that it is the most careful, thoughtful and efficient way of proceeding in this highly complex and technical area.

Industry and other stakeholders need to see the draft legislation, regulations and proposed implementation guidelines in order to understand how the proposed legislation will work. I urge you to consider my recommendation for a broader consultation so that your legislative initiatives can enjoy a timely and successful implementation.

Yours truly,



s.19(1)

CCTA,  
CAIP  
CWTA  
CATAAlliance  
Michael Binder, Industry Canada



November 20, 2002

Paul Pierlot  
Senior Policy Advisor  
Criminal Law Policy Section  
Department of Justice Canada  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, Ontario K1A 0H8

Dear Mr. Pierlot,


On behalf of the Canadian Library Association (CLA) I am sending comments about the Canadian Government's proposal that would force Internet service providers, and other telecommunications companies, to facilitate surveillance of their customers for the police and other intelligence agencies (i.e. the proposed "cyber-crime" and "legal access" legislation). We are writing to voice our concerns that such a proposal, if realized, could gravely jeopardize fundamental principles of privacy in our society, and contradict policies and principles of the library profession, CLA, and other national and international professional organizations to which many Canadians belong.

In 1987, in recognition of the growing trend toward the use of electronic databanks and other electronic means of transferring and storing information, CLA developed a Position Statement to aid in protecting the "personal rights and privacy of users." And in 1994, CLA continued to register its concern over such issues when it referred to privacy in its Position Statement on access to telecommunications. Those concerns remain valid today.

We recognize that, for many years, measures have been taken to protect the privacy and security of Canadian citizens' information, such as the *Canadian Charter of Rights and Freedoms* and Part VI of the *Criminal Code*. However, given the conditions of heightened surveillance and diminishing rights since Sept. 11, 2001, we feel it necessary to call for correspondingly heightened vigilance required to sustain the right to gather and exchange information freely.

We also recognize that the concerns addressed in the proposed legislation derive from the effects of globalization and international agreements such as the Council of Europe's *Convention on Cyber-Crime*. We understand that Canada's role in encouraging the development of electronic information and communication networks and joining other countries in treaties such as NAFTA and WTO has been to encourage greater economic and social freedom and success. Legislation such as that proposed for the sake of national surveillance could provide the opportunity for further objections to such global agreements.

.../2



Canadian  
Library  
Association

328 Frank Street, Ottawa ON, Canada K2P 0X8  
Tel:(613) 232-9625 Fax:(613) 563-9895 [www.cla.ca](http://www.cla.ca)

Canadian Association of College and University Libraries  
Canadian Association of Public Libraries  
Canadian Association of Special Libraries and Information Services  
Canadian Library Trustees Association  
Canadian School Library Association

000180

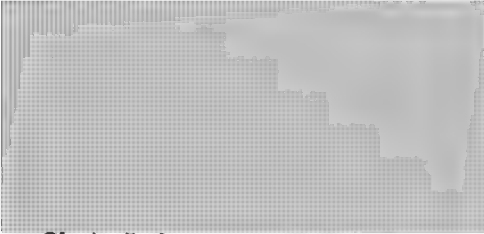


- 2 -

We implore the Government to please consider carefully the potentially deleterious effects of such legislation on Canadian society in general, but also on constituencies such as libraries.

We thank you for the opportunity to voice our opinion on this matter.

Regards,



s.19(1)

Chair, Information Policy Committee



**Cloutier, Marie**

**From:** [REDACTED]  
**Sent:** 2002 Nov 21 6:00 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Lawful Access comments

A few comments:

- The lack of clarity is of a huge concern since the vague new laws and amendments to existing ones leave the door open for things like civil protests and dissident Web sites to be considered illegal.
- This approach doesn't make sense, because the activities the government is using as an excuse for spying on the public are illegal anyway.  
Security and privacy should not necessarily be opposed to each other. Legislation like Lawful Access should not be tolerated by the Canadian public, since we can not and should not accept that protecting us from harm must come at the expense of our privacy. In a white paper written earlier in 2002 Ontario Information and Privacy Commissioner Ann Cavoukian wrote: "Many security technologies can be redesigned to remain highly effective, while at the same time minimizing or eliminating their privacy invasive features."
- Before sweeping and very invasive legislation that's likely to be a burden on the private sector is introduced it may be a good idea to figure out if the law is targeting a real or imaginary threat, says Stein. We may well end up in two to three years with compromised privacy, compromised equality and diminished security.
- A better use of resources would be for the Canadian government to initiate a project similar to the US Homelands Security office's integrated police and security database. Instead of each police department "hoarding" their intelligence data, a mechanism for the secure dissemination of this data would have a far more dramatic impact on security and crime prevention than the Lawful Access proposal.

In my opinion, this proposal is an unacceptable erosion of basic Canadian freedoms that is not acceptable.

Regards,

[REDACTED]  
s.19(1)

Brampton, Ontario  
[REDACTED]

2002-12-11

000182

**Privacy Commissioner  
of Canada**

112 Kent Street  
Ottawa, Ontario  
K1A 1H3  
Tel.: (613) 995-8210  
Fax: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

**Commissaire à la protection  
de la vie privée du Canada**

112, rue Kent  
Ottawa (Ontario)  
K1A 1H3  
Tél.: (613) 995-8210  
Télec.: (613) 947-6850  
1-800-282-1376  
www.privcom.gc.ca

D02-024210

MCUMAN

150002

C.C. J. Normand

J. Boudreau



**NOV 25 2002**

The Hon. Martin Cauchon, P.C., M.P.  
Minister of Justice  
and Attorney General of Canada  
284 Wellington Street, 4<sup>th</sup> Floor  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

I welcome the opportunity to comment on the "Lawful Access" proposals that have been put forward by the Minister of Justice and Attorney General of Canada, the Solicitor General of Canada and the Minister of Industry.

The proposals that have been presented in the consultation paper are of fundamental importance to Canadians. Under the so-called "lawful access" proposal that the federal government has put forward, our use of the Internet and our electronic communications would be subject to unprecedented scrutiny

The interception and monitoring of private communications is a highly intrusive activity that strikes at the heart of the right to privacy. If Canadians can no longer feel secure that their web surfing and their electronic communications are in fact private, this will mark a grave, needless and unjustifiable deterioration of privacy rights in our country.

I do not suggest that privacy is an absolute right. I recognize that there may sometimes be a need for some new privacy-invasive measures to enhance security and allow law enforcement agencies to investigate crimes and threats to public safety. But proposals for any such measures must be evaluated calmly, carefully and on a case by case basis.

The burden of proof must always be on those who claim that some new intrusion or limitation on privacy is necessary.

I have suggested that any such proposed measure must meet a four-part test:

- it must be demonstrably necessary in order to meet some specific need;
- it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;

MINISTER OF JUSTICE  
MINISTRE DE LA JUSTICE  
RECEIVED - RECU

12 NOV 25 2002



- the intrusion on privacy must be proportional to the security benefit to be derived; and
- it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.

The consultation paper cites two main reasons for the measures it proposes:

- a need on the part of law enforcement and national security agencies to "maintain lawful access capabilities" in the face of technological developments; and
- a need to enable Canada to honour its international commitments, particularly the Council of Europe *Convention on Cyber-Crime*.

It is apparent to me, however, that what is being requested here are significantly new and enhanced powers of access to the private communications of Canadians that go far beyond maintaining the capabilities and authorities that law enforcement and national security agencies may have had in the past.

What's missing is evidence demonstrating that there is, in fact, a serious problem that needs to be addressed. Lacking any evidence of serious problems requiring correction by invading the privacy of Canadians, it is not possible to be persuaded that the proposals address these problems effectively, proportionally, and in the least privacy-invasive manner possible.

As a first step, I would strongly encourage the three departments involved in this proposal to present a clear statement of the problems faced, along with empirical evidence supporting the need for enhanced interception and surveillance powers as proposed in the consultation paper. The arguments advanced in the consultation paper are completely insufficient.

I am equally unconvinced by the argument that international commitments require Canadians to submit to an enhanced domestic surveillance regime. This is especially the case because one of the main purposes of the Council of Europe *Convention on Cyber-Crime* is to facilitate information-sharing among law enforcement agencies in the signatory countries. This raises the spectre of intrusive surveillance activities carried out upon Canadians by Canadian law enforcement and security agencies, yet initiated by foreign agencies, for foreign crimes or with regard to other activities that may be perfectly legal in Canada.

Furthermore, it is my understanding that the Council of Europe Convention has not yet been ratified by Canada. Therefore, it would seem that whatever legal obligation is being asserted to implement its provisions is in fact non-existent.

.../3



Very frankly, if the Council of Europe *Convention on Cyber-Crime* requires intruding on the privacy rights of Canadians to an extent that cannot be justified on its own merits and that is inconsistent with our Canadian values and Canadian rights, then this *Convention* should not be ratified by the Government of Canada.

Turning to the specifics of the consultation paper, the lack of detail makes it difficult to establish exactly what is being proposed, although the overall intent, and the threat to privacy, appear clear. Accordingly, I will confine my remarks to the general proposals as outlined in the consultation paper.

### **Technical intercept capability**

Notwithstanding the lack of credible evidence of a serious problem, I recognize that new information and communications technologies may pose a challenge to conventional interception and surveillance techniques. I accept that there may be a need to require telecommunications companies to provide a basic intercept and surveillance capability.

But what is done must be consistent with the consultation's paper insistence that the intent is simply to maintain the status quo by ensuring that existing state powers can effectively be applied to new methods of communication. This means that law enforcement and national security agencies should have the same ability to intercept and monitor e-mail and cellular telephone communications, with the same kind of judicial authorization based on the same criteria, as is now the case with regard to letter mail and conventional telephone communications.

Therefore, it may be reasonable in principle to enhance the current technical intercept capability with regard to e-mail and cellular telephone communications. But because many critical details are lacking in the consultation paper, I must reserve final judgment in this regard pending a better understanding of how the intercepts are to be carried out, by whom and for what purposes and the evidentiary thresholds, oversight controls and safeguards that will be required.

.../4



## Retention and preservation orders

It is good that the consultation paper does not contemplate general retention orders for Internet and cellular telephone data. Requiring all service providers, or even individual providers, to retain data on all subscribers would be an outrageous invasion of privacy. We would not accept a proposal that law enforcement and national security agencies should be able to photocopy the mail of all Canadians or record all telephone calls just in case they may want to look at the mail or listen to the calls at some time in the future. A general retention order would be equally offensive to privacy.

I would strongly urge the government to resist any suggestions that general retention requirements be part of the lawful access initiative.

However, the consultation paper does propose the creation of a "data-preservation order" to act "as an expedited judicial order that requires service providers ... to store and save existing data that is specific to a transaction or client." The purpose of such an order is to ensure that communication service providers, as custodians of communications data, do not delete subscriber-specific information until such time as they are served with a search warrant or production order.

Preservation orders are just as dangerous and inappropriate, from a privacy point of view, as retention orders. As the consultation paper indicates, the concept of a preservation order does not exist in Canadian law. This negates the argument that this type of authority is necessary to "maintain" existing lawful access capability.

Preservation orders would enable law enforcement and national security authorities to require wireless telephone services and internet service providers to preserve detailed records of every telephone number we called, every Web site we visited, every page of that Web site we read, what we searched for and downloaded.

The consultation paper does not make it clear what level of proof of suspected wrongdoing would have to be presented to a judge in order to apply for, and serve, such an order on communication providers. Indeed, in some circumstances, no judicial involvement at all would be required; law enforcement or national security authorities themselves would simply be able to issue a preservation order.

The dangers inherent in this become even clearer when we consider that preservation orders could be served on ISPs to require them to retain the *content* of their subscribers' correspondence passing through their networks. That is, a preservation order could very well become a backdoor way to conduct interceptions, via a third party, without any of the judicial safeguards and remedies associated with interception warrants.

.../5



Nothing in the consultation paper denies that communications content might be captured in this manner. Indeed, another proposal in the paper suggests that communications content, such as in e-mail messages, when "preserved" and stored in recorded form, is arguably subject to a search warrant which is considerably less onerous to obtain.

The privacy implications of preservation orders are further compounded by the involvement of neutral third parties, i.e., the communication service provider, with all that this implies for data security and the potential for unlawful access by hackers and others.

### Production orders

The consultation paper proposes the use of "production orders" to compel the custodian of documents to deliver or make them available to law enforcement officials within a specified period of time. Except for a very narrow type of production/collection order, there are currently no production orders provided for in the *Criminal Code*. Two different production orders are contemplated. Each applies to different types of information:

- A "general production order" would function in a similar manner to a search warrant. A major difference is that the physical presence of a law enforcement officer to conduct the search is not required.
- A "specific production order" would apply to "telecommunications associated data" or "traffic data" which is, arguably, subject to a lower expectation of privacy and thus a lower judicial standard for law enforcement/national security access.
- The paper also asks whether there is a need for a second type of specific production order that would apply to customer name and address and service provider information. (I will deal with this issue separately below.)

Again, the paper does not make the case for production orders—the need has not been demonstrated.

More specifically, I question the assumption in the paper that "telecommunications associated data" necessarily involves a lower expectation of privacy. The paper assumes that the traffic data generated by wireless telephone service, e-mails, or using the Internet is analogous to a record of the telephone numbers called or received from a particular number.



In the world of wireless telephony, "traffic data" also includes a record of the location of the cell phone in question as it moves about from cell to cell. For this reason, the traffic data generated by wireless calls is far more personal and revealing.

In the Internet world, traffic data would encompass the e-mail addresses on all correspondence to and from the subscriber, a record of date, time, and size of message as well as other pertinent (but unnamed) transmission details but excluding message subject and content.

And, as previously noted, Internet "traffic data" also encompasses a record of every login session, every web page visited and read, every search term entered, every file downloaded, every purchase made, and so forth—in short, virtually the entirety of one's online "session" but excluding the content of email messages.

Although the proposals outlined in the consultation paper purport to adapt or maintain law enforcement access to communications data, it is clear that this new instrument will go far beyond accessing a simple record of numbers called or received to include very intimate details and a much larger profile of our activities, thoughts, preferences, and lifestyle.

For this reason, I take issue with the assertion that this kind of data would or should be subject to the same (lower) expectation of privacy as the information generated by wireline telephone calls. What is contemplated here is an enormous expansion of access to a large and growing reservoir of data created by communications subscribers.

Given all these considerations, I am not persuaded as to the need for, nor the acceptability of, creating new instruments in the form of retention orders and production orders.

Agents of the state in Canada cannot order Canada Post to photocopy the address on every envelope we send, nor can they order bookstores to keep a record of every book we buy, let alone of every page of every magazine we leaf through. There is no reason why they should be able to exercise such powers with regard to every e-mail someone sends or every Web site he visits.

The two-step process that is proposed - allowing law enforcement and national security authorities to obtain first a preservation order and then a production order - also itself carries a risk of eroding the current standards that must be met when agents of the state seek judicial authorization to invade communications privacy.

...17





If a judge is asked only to authorize an order to "preserve" communications data, with the issue of actually "producing" that information into the hands of authorities being left for later judicial determination in a subsequent proceeding, he or she may be less inclined to insist on a high degree of satisfaction that this order is actually necessary. And, likewise, the second judge who is asked to order the actual production of the data may be more inclined to assume that the appropriateness of the whole intrusion must already have been demonstrated to the judge who approved the original retention order.

My view is that if the police or security services want to examine the online or wireless communications of any individual whom they suspect of serious wrong-doing, they should only be able to do so in the same manner that now exists with regard to other forms of communication. They should be required to obtain a judicial order, based on the same standard of proof as applies to other forms of communication, authorizing them to intercept that individual's online or wireless communications.

There is no doubt that this would be more onerous, more time-consuming and more labour-intensive than the retention order/production order technique that is proposed. But that is precisely the point: Invading the privacy of Canadians to an unprecedented extent should not be made so convenient or so easy as to encourage the carrying out of such activities on a wholesale basis rather than only in the most serious and unavoidable circumstances.

### **Customer name and address and service provider information**

The consultation paper notes that with the deregulation of the telecommunications market, law enforcement/national security agencies are experiencing difficulties in identifying the local service provider associated with a given telephone number. The paper also refers to problems obtaining customer name and address information.

The paper suggests that it might be appropriate to create a national database containing customer name and address and service provider information for all Canadian telephone subscribers—as recommended by the Canadian Association of Chiefs of Police.

I cannot support the creation of such a database. Yes, it would make it easier for law enforcement/national security agencies to obtain customer name and address and service provider information, but the difficulties involved in obtaining this information can hardly be insurmountable. Furthermore, these difficulties serve a purpose—they force law enforcement/national security agencies to think twice before seeking to obtain this information.

.../8



The consultation paper appears to endorse a view that the name and address of an individual with a given telephone number carries such a low expectation of privacy that access to it by law enforcement authorities should be a routine procedural matter. I take issue with any assertion that one's name and address, when associated with a unique identifier like a telephone number, is somehow unworthy of privacy protection.

In consequence, I see no compelling reason to change current law and practice regarding access to this information.

Carrying this idea a step further, the consultation paper floats the possibility of all service providers being obliged by law to collect and verify the identity and address of all subscribers. This raises the spectre of convenience store clerks demanding and recording—and then transmitting—people's sensitive personal information, such as driver's license and credit card numbers, as a condition of purchasing pre-paid phones or phone cards. This would be a gross invasion of privacy.

I am likewise opposed to the idea of creating a centralized national database registry of Internet subscribers. If this were established, as has been proposed for the telephone database noted above, law enforcement authorities could automatically and routinely trace an Internet Protocol address back to the registered user, circumventing the normal due process of requesting this information from each ISP on a case-by-case basis. Such a project, if carried out, would effectively obliterate any expectation of privacy and anonymity on the Internet.

## Conclusion

As I have indicated, the consultation paper does not demonstrate why these measures are necessary. This is all the more troubling because the measures being contemplated go far beyond simply maintaining existing capabilities and authorities.

On this issue, my position is simple. I do not see any reason why e-mails should be subject to a lower standard of protection than telephone calls or letters. And I do not see why Internet browsing should be subject to a lower standard of protection than book purchasing or researching in a reference library. Canadians should not be subject to greater monitoring or scrutiny just because they choose to use new communications technologies.



In a free and democratic society like Canada, the interception and monitoring of private communications carries extraordinarily strong symbolic and psychological implications, in addition to the obvious practical ones. Canadians are entitled to feel confident that their communications and on-line activities will not be arbitrarily intercepted or scrutinized.

Yours sincerely,

A handwritten signature in black ink, appearing to be 'G. Radwanski'.

George Radwanski  
Privacy Commissioner of Canada

c.c.: Hon. Wayne Easter, Solicitor General of Canada  
Hon. Allan Rock, Minister of Industry



Ministry of the  
Attorney General

Ministère du  
Procureur général

Assistant Deputy  
Attorney General  
(Criminal Law Division)

Sous-procureur  
général adjoint  
(Division du droit criminel)

720 Bay Street  
6th Floor  
Toronto ON M5G 2K1  
Phone: (416) 326-2616  
Fax: (416) 326-2063

720 rue Bay  
6th Floor  
Toronto ON M5G 2K1  
Télé: (416) 326-2616  
Téléc.: (416) 326-2063

November 26/2002

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor,  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

Re: Lawful Access - Consultation Document

In the above-noted consultation document, you asked for comments to be submitted by November 15, 2002. I understand that that deadline has now been extended to December 16, 2002.

There has, however, been a more detailed consultation process between federal and provincial officials on the subject of potential lawful access legislation going back to 2001 that recently continued with a day-long meeting here in Toronto on November 12, 2002, at the conclusion of which the prospect of further discussions was raised. We have been and may continue to convey our views on lawful access at a staff level through this process. While not formally commenting on the original, more general consultation document, we may or may not put some thoughts in writing at the staff level at a future date.

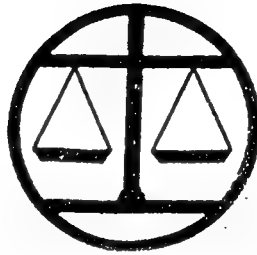
Yours very truly,

s.19(1)



Assistant Deputy Attorney General –  
Criminal Law

**CIVIL LIBERTIES ASSOCIATION,  
NATIONAL CAPITAL REGION**  
FOUNDED 1968



**ASSOCIATION DES DROITS CIVILS,  
RÉGION DE LA CAPITALE NATIONALE**  
FONDÉE 1968

s.19(1)

22 Third Ave., Ottawa, Canada, K1S2J6, Tel. 613-520-2600 #3797, 520-3962 (FAX)

Internet: [www.ncf.ca/civil-liberties](http://www.ncf.ca/civil-liberties); e-mail: [REDACTED]

Civil Liberties Association,  
National Capital Region  
22 Third Avenue  
Ottawa ON K1S 2J6

December 2, 2002

Mr. Paul Pierlot  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, ON K1A 0H8

Dear Mr. Pierlot:

### **Lawful Access Consultation**

The Civil Liberties Association, National Capital Region is pleased to provide the attached submission on the Consultation Document on Legislative Proposals on Lawful Access.

The document was prepared by Leo Lehtiniemi, who participated in the October consultation meeting. It has been reviewed by our full executive. We trust that our comments provide constructive assistance to the Lawful Access team.

We appreciate having had the opportunity to participate in the consultation process. We would be interested in taking part should there be any follow up in response to the submissions that have been prepared.

Please do not hesitate to contact me (520-2600 Ext 3797, fax 520-3962) if you have any questions about the attached document.

Yours truly,

President

[REDACTED]  
Attachment:  
Consultation Document on Legislative Proposals on Lawful Access

**CIVIL LIBERTIES ASSOCIATION,  
NATIONAL CAPITAL REGION**  
FOUNDED 1968



**ASSOCIATION DES DROITS CIVILS,  
RÉGION DE LA CAPITALE NATIONALE**  
FONDÉE 1968

22 Third Ave., Ottawa, Canada, K1S2J6, Tel. 613-520-2600 #3797, 520-3962 (FAX)

Internet: [www.ncf.ca/civil-liberties](http://www.ncf.ca/civil-liberties); e-mail: [REDACTED]

## **LAWFUL ACCESS CONSULTATION**

### **SUBMISSION ON LEGISLATIVE PROPOSALS**

By [REDACTED] s.19(1)

On behalf of the Civil Liberties Association, National Capital Region  
December 2, 2002

#### **INTRODUCTION**

1. The Civil Liberties Association, National Capital region is grateful for having been invited to participate in the consultation on lawful access. We applaud the Department of Justice, Industry Canada, and the Solicitor General Canada for seeking input from a broad spectrum of perspectives in Canadian society.
2. We acknowledge and deplore the possibility that terrorist acts may be directed at critical facilities and the Canadian population, and realize the need for heightened vigilance and security to detect and prevent terrorist activities and the need to deter major crime in Canada.
3. We recognized that criminal and terrorist elements make use of rapidly evolving electronic communications technology to plan, finance and execute actions that may be harmful to Canadians.
4. We appreciate that enhanced powers of lawful access may assist security and law enforcement authorities in their preventive efforts directed against terrorists and the perpetrators of major crimes.
5. We note, however, that the vast majority of citizens are neither involved in major criminal activities nor do they support or participate in terrorism.
6. We note that although many Canadians may share behavioural, demographic and/or cultural characteristics and attributes that may be associated with groups that are known or believed to be involved in major criminal and/or terrorist activities, the vast majority of these citizens in no way approve of, support, assist or participate directly or indirectly in criminal or terrorist activities.
7. We note that despite what is desired or intended in any human endeavour, surprises are encountered, mistakes do happen, and things do go wrong. Unintended effects are inevitable. Murphy's Law is an Iron Law.

8. We are concerned that any new or increased powers to assist law enforcement and security authorities protect Canada and Canadians from major crimes and/or terrorist acts do not subject innocent citizens to suffering or loss of the very rights and freedoms that are threatened by major crimes and terrorism.

9. We believe there is need for vigilance at the highest level against indiscriminate application, error, misuse or abuse of lawful access powers, and for tangible controls and criteria to protect against that.

10. We stress the importance of ensuring that legislation to confer any expanded powers will include suitable provisions which: a) serve as effective safeguards against unintended or inappropriate use of those powers; b) prevent and deter unwarranted use of those powers by security and law enforcement authorities that adversely impacts on the civil rights and liberties of Canadians; and c) allow timely remedies for citizens who have fallen victim to indiscriminate application, error, misuse and/or abuse of increased security and law enforcement powers.

## GENERAL OBSERVATIONS AND COMMENTS

### A. BALANCE

The Lawful Access Consultation Document (August 25, 2002) identifies the public policy need to balance the rights, privacy, security and economic well being of all Canadians. That implies the need to ensure that law enforcement and security enforcement powers respect rather than overlook civil liberties and human rights.

Apart from acknowledging that need, however, the Consultation Document pays scant further attention to human rights and civil liberties. It is devoted primarily to matters of what enforcement powers are needed and how that might be achieved, including what technical capabilities service providers should be required to have or acquire and what compliance mechanisms may be necessary. The primary focus is on enabling and empowering law enforcement and security authorities. There is little specific consideration directed to how the civil liberties and human rights of Canadians will be respected, safeguarded and protected. The topics of safeguards against inappropriate use, errors, misuse and abuse by authorities, and of managing and controlling authorities in the use of new powers, are absent.

The Civil Liberties Association, National Capital Region raised concern at the October 21 consultation session about this selective emphasis on the legal and technical aspects of the proposed legislative changes that is evident in the Consultation Document and the Agenda. We suggested there was need for greater balance, and a need to give greater attention and consideration to issues of civil rights and liberties. Other participants expressed support. We believe this imbalance must be redressed.

Our focus centres on the possible impacts of the lawful access proposals on personal privacy and human rights and freedoms, and on the need to pay the strictest attention in any legislative proposals to safeguard hard-won rights and freedoms that characterize our democratic and free society. We believe that Canada should exercise the utmost care to not take any measures that move the yardsticks back, and make every effort to ensure that Canada retains its position of international leadership in civil liberties and human rights. Our comments are to that end. We also offer more general comments on other aspects of the Consultation Document.

## B. NEED

A critical and continuing challenge facing lawmakers is to correctly identify and assess the magnitude and severity of problems and their likely impacts before they legislate solutions. Laws are usually intended for the longer term. Over time, an inappropriately crafted statutory instrument can have unintended consequences and side-effects. These can create problems that outweigh the resolution of the purported problem the legislation was intended to rectify or attenuate. Yet, once legislation has been adopted and resources, personnel and infrastructure have been put in place, it becomes difficult to make corrections. Operations and procedures become standard practices that get integrated into other processes in society. It becomes rather hard to corral, rein in, dismantle or withdraw powers that have been granted by statute. The need for a rigorous front-end appraisal is vital.

While there is an unquestionable need for precautionary measures to counter terrorism, it is important to guard against judgement being clouded and actions being propelled by a climate of need and urgency driven by what "might be possible". The rationale for expanding access powers of law enforcement and security officials should be based on robust and compelling evidence to support proposals for those expanded powers.

Protection against a perceived, potential or theoretical threat is not readily demonstrable and quantifiable - it can be a bogey-man based on a magnified or managed climate of fear. Yet although the level of real risk may be not be great, the consequence of error can be enormous. It is thus hard to determine what is really needed, and how much security or law enforcement will be enough. Fortunately, the incidence of terrorist acts in Canada in the recent past is low. And while the consequences of terrorist acts can be dramatic and tragic, the reality is that these events are less common in Canada than are accidents by law enforcement personnel that result in physical injury and death.

A questionable focus may underlie the "need" for the proposed new lawful access measures. It appears, at least in part, to be predicated to some extent on a desire by law enforcement and security authorities to keep pace with rapid changes in the communications field and with their international colleagues. While the desire to keep pace with the rapid evolution of technologic capabilities is understandable, it warrants considered scrutiny.

The proposed lawful access provisions propose a commitment to, as a goal in its own right, a continuing requirement to modernize existing capabilities whenever technical limitations arise. Trying to maintain currency with the cutting edge of technology is much like chasing a shadow. There are examples of officials ordering newer and more modern equipment while existing equipment was used to only a fraction of its capability. A commitment to "keep up" can become a black hole with a growing and insatiable appetite for resources. In addition, it may carry an opportunity cost in terms of diverting and drawing attention and resources away from other areas of equivalent or greater need.

We are of the view that the notion of fail-safe law enforcement and security is an illusive and unattainable ideal. There can never be enough done to thwart all evil efforts. Resourceful and committed individuals will always find some way to avoid or bypass security measures. A great deal of sound and informed evidence-based judgement is required.

We suggest a disciplined and methodical risk analysis is needed to demonstrate that other compelling matters are at stake and underlie the identified needs for expanded lawful access. That exercise would require: clarifying the nature of the actual problem(s) that must be addressed; quantifying the severity and generality of each; assigning realistic probabilities of their occurrence;



4specifying how the proposed expanded powers of lawful access will actually manage, suppress, reduce or eliminate the problem; and estimating the anticipated ranges of consequences, including both the benefits and the costs, of implementing the proposals compared to relying of available powers. A sensitivity analysis should be included for each of these elements. In the event that analyses of risk, benefits and costs have already been done, it would be prudent to scrutinize the methods, assumptions and data used to confirm their rigour and validity.

### C. DANGER OF POTENTIAL FOR ERROR

We are fortunate that the proposed new powers of lawful access are for situations that are not commonplace in Canada. On the other hand, the new and expanded lawful access proposals invite accidents that could have broad impacts on the privacy, civil liberties and freedoms of Canadians. We are of the view that the need for safeguards for civil liberties, personal privacy, and human rights and freedoms is of equal importance as is the need for physical and material security.

It is germane to consider the concepts of "false positives" and "false negatives" that are employed in statistically analysing the effectiveness and efficacy of drugs, treatments, screening tools and other applications. These concepts arise from an accumulated knowledge that most things seldom, if ever, work perfectly. The duds that sometimes slip through quality control tests are examples of false positives. The proverbial baby that might have been tossed out with the bath water represents a false negative. False positives and false negatives are things that should not happen if everything worked perfectly, but it often does not. The probability of each type of error is variable, but they are related. In general, the more stringent the acceptance criteria to minimize false positives, the greater the number of false negatives, and vice versa.

To illustrate, one can consider fishing nets used by trawlers. If the purpose is to avoid taking undersized fish, which would be false positives, a large mesh net will be used. If one is to believe the fisheries experts, this should be the standard practice if one wishes to conserve viable fish stocks.

In this situation there is a high probability that some, and perhaps even many fish of acceptable size will slip through and be lost. They are false negatives.

In contrast, if the purpose is to make sure that one catches all the fish of eligible size, and to avoid letting any eligible fish slip through, a smaller mesh net will be trawled. In that situation, the number of targeted fish that get away may indeed be reduced, but there will be a commensurate increase in the number of undersized fish that are caught. Because there are penalties associated with being caught with undersized fish in possession, these fish - false positives caught by the net - are undesired. They are dumped overboard, but they often die from having been subjected to the experience of being caught. In fact, finer-mesh nets sometimes become so overloaded with too many fish of both desired and undesired sizes that they burst. Fisheries experts suggest that the use of undersized nets is a major reason why stocks have been depleted and our fisheries are in collapse.

The example of fishing nets is a relevant analog to the lawful access proposals. Our legal tradition is one that has shown great sensitivity to avoiding false positives, and tolerating and accepting false negatives as a justifiable price of protecting the innocent from wrongful punishment. It is succinctly expressed in the adage "Better to let 100 guilty persons go free than to convict one innocent person." It is a corner stone of our legal system.

The current climate of anxiety about terrorism is one in which security and law enforcement spokespersons may be tempted to encourage or even foster public fear to shore up their bids for

increased resources and powers. One must consider that those spokespersons have a vested interest in emphasizing the seriousness of the threat, the severity and magnitude of the consequences of security and law enforcement failures, and the importance of their roles and responsibilities in protecting the public. By virtue of their mission in society, they are obliged to make efforts to obtain whatever statutory authorities and resources they believe are needed to protect our physical and material security. Given their responsibilities, their primary focus has been and probably must be on minimizing or avoiding false negatives.

However, that focus has been shown in past situations such as the 1970 FLQ crisis to carry an expense of many false positives. Because non-disclosure agreements are a condition of many mediated settlements, the public will never know the total direct costs of many of these mistakes. It is unlikely that even the full knowable costs of locating and apprehending "suspected separatists", their temporary incarceration, and the associated legal expenses incurred by public institutions have ever been tallied. We are aware, though, that the Quebec government paid some compensation to those falsely arrested in the October 1970, crisis.

We will never be able to monetize the non-visible human costs, such as the psychological shock of loss of human dignity, individual personal security and freedom of movement, that were inflicted upon those who were arrested and later let go without being charged. It helps one realize the enormity of the situation if one considers that the apprehension of 600 Canadians in that incident is proportionally many times greater, given the size of our population, than the estimated 1000 currently believed to be held by American authorities in connection with possible ties to terrorism.

It is critically important to keep in mind that errors are made. Murphy's law is an Iron Law. If any expanded lawful access proposals go forward, they must recognize and adequately address the likelihood of error. It is a broadly accepted imperative in Canadian society that the side-effects of a cure should not be worse than the illness. Care must be taken that the measures to protect physical and material security are not introduced at the expense of diminished or sacrificed civil liberties and freedoms.

With that in mind, the legislative proposals must include provisions that specify what explicit measures will have to be taken by law enforcement, security and legal authorities to respect the privacy and civil liberties of Canadians. They need to include provisions specifying what structures, mechanisms and procedures must be put in place to ensure that all specified measures are taken and are then maintained inviolable. There will also have to be provisions that address what will be done when mistakes are made and things go wrong. These include both identifying repercussions for inappropriate use, error, misuse or abuse in the execution of powers and authorities, and mechanisms and procedures to allow timely remedies and restitution for innocent victims after things have gone wrong. Finally, there is need to specify oversight and accountability mechanisms to control against abuse of powers that do not respect individuals' civil rights and freedoms, privacy and security against unwarranted interference by law enforcement and national security agencies. These are discussed in greater detail below.

#### D. NEED FOR BUILT-IN LIMITS AND CONTROLS

The Consultation Document pays no attention to the need for explicit provisions to discourage and counter indiscriminate application, errors, misuse or abuse by those individuals authorized to use the proposed new powers. Even in the best of times mistakes do happen, and well-intentioned actions do go wrong. One can predict with certainty that the incidence of unintended consequences will increase in times of perceived or anticipated crisis and increased vigilance in a climate of fear of possible terrorist acts. There will be cases of over-zealousness, hastiness and excessive erring on

the side of caution that will result in the application and use of lawful access powers that subsequent review will clearly show to have been inappropriate and unwarranted, and to have constituted unnecessary violation of or infringement upon the civil rights and liberties of innocent Canadians. To guard against such abuses, there is a need to embody specific and explicit conditions and safeguards in whatever legislation is introduced. This has a dual purpose. In the first instance, including such provisions makes clear that suitable protections of civil liberties exist and are formally recognized in connection with powers of lawful access. This will eliminate uncertainty and will both remind and sensitize those focussed on fighting terrorism, major crime, cyber-crime and organized crime to the framework of civil rights, freedoms and liberties that characterizes Canadian society. In the second instance, the articulation and inclusion of specific provisions will help ensure that lawmakers, members of the judiciary, and Parliamentarians and other officials responsible for oversight keep these rights squarely in mind when reviewing matters relating to the exercise of lawful access.

#### E. NEED FOR SPECIFIED REPERCUSSIONS FOR INAPPROPRIATE APPLICATION

Events regularly draw attention to the harsh reality that mistakes are unavoidable, in all domains, even when the best of intentions are present. Particularly dramatic events, such as the recent rescue of hostages in a Moscow theatre effected by Russian special forces command public notice and receive high media profile. Less dramatic incidents occur with far greater frequency and regularity, but pass without receiving prominent attention. Incidents such as those where an individual's assets are frozen because a foreign state has unproven suspicions about their activities, and those where innocent people are killed in accidents involving high speed pursuits fade into obscurity fairly quickly.

We are often reminded that we do not live in a perfect world. We are aware that there are real and grave threats to our property and our personal security. We recognize that there may be exceptional circumstances where it is reasonable to err on the side of caution to prevent possible terrorist acts or to protect us from major crimes. However, we are equally concerned that there is need for precautions against errors, misuse and abuse by our protectors, especially in a climate of heightened anxiety.

The Criminal Code contains some provisions against malfeasance and abuse of authority on the part of officers of the law. The extent to which these would apply to inappropriate use of lawful access is unclear and untested. At best, the more general applicability of existing clauses in the Criminal Code to proposed lawful access provisions remains too uncertain to provide reassurance that they would have any effect to discourage going too far, too broadly, or too quickly in the exercise of the proposed powers. What is needed are specific provisions with appropriately harsh consequences for unwarranted and inappropriate use, errors, misuse and abuse of each of the proposed new or extended powers of access. That will communicate a clear and unambiguous message about the nature of the balance to be maintained between security and civil rights and freedoms.

#### F. REMEDIES AND RESTITUTION

The focus of the Consultation Document is one-sided. It looks at what powers and measures authorities may need, and how these might be achieved. It looks at what those who will be subject to the proposals may have to do to comply, and what challenges may be faced in the process. It is silent on compliance on the part of authorities and the consequences of their non-compliance. The total emphasis is on what it intends to achieve by way of lawful access. As noted earlier it ignores

possible errors and their impacts on the service provider industry and on Canadians whose rights may be infringed or violated. As an inevitable consequence, it pays no attention to the need to identify what restitution will be made to those law-abiding individuals who have been wrongfully victimized by officials exercising these new sought-after powers without due caution and restraint.

We are mindful that those who have been unjustly affected by actions have recourse to the legal system, and recognize the importance of the judicial process in defending the rights and freedoms of Canadians. It is, however, instructive to examine how fully one can rely upon that avenue. We draw attention to the burdens of time, cost, and anxiety that must be borne by those who seek legal recourse through the Courts. For many, these represent hurdles that tax and diminish their enjoyment of everyday life. We note, further, that the design of our legal system implicitly acknowledges the reality that errors are made and will be made in our courts. That is the very reason why various levels and avenues are provided for appeal. Even in the legal arena, things do not always work perfectly or as intended. We note, that despite the availability of these built-in safeguards, justice is not always assured. This is evidenced by the work of the Association in Defence of the Wrongfully Convicted. The Chief Justice of the Supreme Court of Canada has publicly acknowledged the fallibility of our justice and legal systems.

One must look for better alternatives than simple reliance upon the Courts in the usual manner to seek remedy from errors by authorities. We noted earlier the importance of articulating and embedding in any enabling or empowering statutory instrument clear and unambiguous consequences of inappropriate use, error, misuse or abuse of the proposed powers by law enforcement and security authorities, as a deterrent to discourage unwarranted violations of the rights and freedoms of Canadians.

However, we recognize, that by itself, that would be insufficient. There will still be mistakes. There remains a need to include provisions that will allow those who have been wrongly affected and who seek justice to be able to avoid the need for protracted litigation to exercise that right. We believe that to demonstrate and give effect to a balance between the need for security and law enforcement and the need to respect and protect the rights and freedoms of Canadians, it is important to articulate and embed in the enabling or empowering statutory instrument an expeditious recourse and the remedies available to those upon whom error, misuse or abuse was inflicted, but could have been avoided had reasonable precaution been exercised.

## G. OVERSIGHT & ACCOUNTABILITY

The consultation document pays no attention to the need for structured and regular arms-length oversight and public accountability. Law enforcement activities are not above the law - they too must be subject to the law. Law enforcement is carried out by ordinary people, and the propensity for mistakes, both inadvertent and inexcusable, is just as great in the field of law enforcement as it is in any other field of human activity. The halo effect created by virtue of the affiliation of law enforcement and security officials with the justice system should not serve as an umbrella that shelters them from scrutiny and the rules of law. A watchdog function over the exercise and use of any new or expanded powers of lawful access is essential.

There may be a credible and valid need to maintain secrecy about certain highly sensitive matters. There is no question that the nature of some circumstances will compel a need for secrecy in the interests of national security or protecting the integrity of investigation. But one must not allow a claimed need for security to be used as a cover to hide non-sensitive (at least with respect to national security) but embarrassing information needed for accountability and governance. The valid need for security must be balanced by regular disclosure and scrutiny of all other operational information

by arm-length overseers who represent and report to the Canadian public.

## COMMENTS RELATING TO SPECIFIC ISSUES IN THE CONSULTATION DOCUMENT

### a. Council of Europe Convention on Cyber-Crime

The explosion of technological innovation in communications allows criminals and terrorist to ignore geopolitical borders. That makes it increasingly important for security and law enforcement agencies to cooperate more closely and to better integrate their efforts. The Convention on Cyber-crime arises from this trend.

However, the fact that 33 countries have signed the Convention does not automatically mean that Canada has to introduce new lawful access powers to match those in other jurisdictions. Because others are doing it is seldom a necessary and sufficient reason in its own right for one to do something. Many international agreements are not ratified by all nations, and ratification, when it does occur, may take many years to happen. Delay often arises from a need to reconcile and integrate the desired changes with existing realities within individual participating nations. It is parallel to the complexity involved in putting into place national programs in Canada, where inter-provincial differences in the actual nature and level of need, legislative and institutional structures, as well as resources and other capabilities, must be accommodated.

We do not question whether Canada should make changes to allow it to be in a position to ratify the Convention on Cyber-crime. However, it is our view that the matter warrants careful review before Canada takes the requisite actions, such as expanding lawful access, to allow that to be done. Our concern is to ensure that adopting measures used in other jurisdictions does not place the civil liberties, freedoms and Charter rights of Canadians at risk.

Before deciding to expand lawful access powers, there is a need to critically examine and assess a number of issues. In particular, there is a need to assess the civil liberties and human rights frameworks, practices and traditions of those countries that have signed the Convention on Cyber-crime. One must scrutinize and weigh whether there are critical differences in the legislative foundations, judicial structures and processes with respect to the civil liberties, freedoms and rights of citizens of those states that have ratified the Council of Europe Convention on Cyber-crime. This may reveal reasons against integrating too quickly, too widely or too closely. From a civil liberties perspective, there is a need for caution and vigilance in assessing whether certain Canadian values might be placed at jeopardy by seamless integration and the open exchange of information that would soon follow. If there are significant differences between Canada and other countries with regard to the value placed on civil liberties, there may be valid and compelling reason for caution and for delaying action to protect Canadians from being subjected to others' standards.

There is also a need to objectively compare the actual conditions that exist in other countries and the levels of the actual problems and demonstrable threats that they must deal with. This includes examining what other tools are and are not available to law enforcement and security officials in other countries, and looking at what ancillary or alternative means are available through their military intelligence and covert services. The need to harmonize does not necessarily mean the need to imitate or duplicate. Despite the desire to cooperate, we must not lose sight of the value of fences and firewalls that protect Canadians from authorities in other countries that do not have the same protections for civil liberties and freedoms that we have.

#### b. Intercept Capability:

The focus of the Lawful Access Consultation Document is focussed almost exclusively on what authorities wish to accomplish and how they might do so. There is a need to balance this with more detailed consideration of safeguards against the incidental or accidental "collateral" damage to privacy and civil rights and freedoms.

In our view, specific and explicit protections against infringements upon civil liberties and human rights must be built in to any statutory provisions to enhance intercept capabilities and powers of security and law enforcement agencies. These protection provisions should be of broad and general application, and not vulnerable to being easily set-aside, superseded or preempted by other legislated powers. This is especially important in any legislation under which authority can be delegated to a working level, where the focus is of necessity on operational matters, and not on broader policy issues and implications, and where the responsibility and process for making regulations does not allow for full scrutiny.

The reason for safeguards against interception will not be as obvious as other violations of civil liberties, such as unlawful detention. It is essential to bear in mind that freedom of expression will be greatly curtailed through self-censorship if people come to expect routine monitoring of their communications by law enforcers. Completely innocent people may self-censor based on recognizing the possibility of misinterpretation by some monitoring body. The upshot can be a profoundly different society than the one we now enjoy.

#### c. Amendments to the Criminal Code

To even consider anticipatory orders raises grave concerns about invasion of privacy and fishing expeditions. It invites abuse based on grounds such as racial profiling that violate the Charter and core Canadian values. We cannot accept these.

#### d. Virus Dissemination

To allow criminalizing actions that have not taken place opens a door that is fraught with danger. It denies that there can be and often is an exercise of better judgement whereby contemplated or fantasized actions are never carried out. If this door is opened, where will it stop? To allow anticipatory orders raises the spectre of regimes where those who even dared to openly wonder about policies, positions and possibilities other than the official party line were judged to be enemies of the state. Quite simply, it is a first step that can lead to somewhere that Canadians should not want to go.

#### e. Interception of E-mail

The proponents of expanded lawful access posit that less stringent controls over interception of e-mail are justified on the basis of a lesser expectation of privacy. This appears to be premised on the assumptions that because some technically sophisticated would-be snoopers (including security and law enforcement authorities) know how easily e-mail can be accessed, then all Canadians are aware of its porosity and vulnerability to access, and that those who use that communication medium therefore implicitly accept those limitations on the privacy of their e-mail communications. Canadians cannot consent, implicitly or explicitly, to interception of their e-mail unless they are



aware that it can be done, and how and where it can be done.

It is not possible to assess if there is a lesser expectation of privacy on the strength of whether one takes precautions to ensure that their e-mail communications will not be intercepted. The act of taking precautions to prevent interception demonstrates an awareness that e-mail communication can be and possibly will be intercepted, and the desire to avoid allowing that to happen. Those who do not take precautions may be indifferent about vulnerability to third party access, or they may simply be unaware. One cannot presume or construe that all Canadians who trust that others will not snoop, and those who are ignorant of what interception capabilities are possible, are in any way accepting of those interceptions, and hence have a lower expectation of privacy. That snoopers and would-be snoopers know what is possible for them to do with respect to intercepting e-mail is not a valid basis to believe that everyone knows what is possible.

It is far more likely that the beliefs and expectations of non-technically aware Canadians are based on and informed by their next-closest experience. E-mail is electronic mail, but it is mail. The understanding is that what has changed is the means of transmittal, but what is transmitted is still mail in other respects. The non-technical lay-person in Canada has no reason to believe that the authorities will treat their e-mail any differently than their old postal mail. They know that if some unscrupulous parties open or steal their letter mail, they can call upon the authorities to investigate and prosecute that as a criminal act. If any expectation is reasonable, it is that the authorities would extend the rules about their letter mail to embrace their e-mail, and provide the same protections and sanctions to protect its privacy.

It is also erroneous to assume that those Canadians who have some awareness and knowledge of what is technically possible would find it acceptable for the authorities to do what is possible. Although many know that others might tap into their e-mail, they think it is unethical and that those who do it should be subjected to censure. Law enforcers may sometimes avoid such censure, but only if they follow recognized and accepted procedures, such as obtaining permission from a judge on reasonable legal grounds. It is our view that any information obtained by interception of e-mail which is revealed to other parties should be subject to punitive legal sanctions unless there are special demonstrable circumstances that justify the action. The same standards as are applied to letter mail, which is also highly vulnerable to intercept but which is legally protected, should be applied to e-mail.

#### f. Subscriber and Service Provider Information

There is a long-standing high degree of belief in the value of data bases. Their potential usefulness is beyond dispute. However, their limitations, shortcomings and drawbacks are usually overlooked or downplayed. These are significant, but only come to light periodically. One example is the recent revelation that Canada's Social Insurance Number data base contains in the order of six million more entries than there are eligible Canadians. But in addition to duplicate, outdated, and phony records, data bases may contain inaccurate information in individual records. There can be no doubt that the integrity of SIN data base suffers from incomplete and incorrect records that have not been publicized.

Data bases commonly have flaws other than those having to do with the validity of the records they contain. Among these are errors arising from variations and changes in record layouts over time and across jurisdictions, missing data elements, and incorrect entries arising from clerical and other input errors. The problem of corruption of a data base, where internal programming bugs electronically change the actual location and value of data elements, is one that is known to have occurred, especially in larger data sets.

There are also errors of omission. When critical records are missing, the next closest records may attract attention - attention that is totally unwarranted and unjustified. Alternatively, the absence of records may mean that the data base is incapable of providing the very capability upon which its existence was premised. Neither situation serves us well.

Rather than enumerate other errors, suffice it to observe that all of them represent threats to the integrity of data bases, which can lead to negative consequences with civil liberties implications. The danger arises when imperfect data bases are used as the basis for actions that impact on citizens in a way that prejudices their interests. When the information is not accurate, an inappropriate intervention may take place either as a direct personal action, or covertly without the individual's knowledge. The latter type of situation is particularly insidious, but both carry a potential for inconvenience and even harm. Anyone who has travelled in a police state and has experienced being stopped to show papers and explain one's reasons for being there will appreciate the unpleasant psychological reaction that comes from being confronted with what seems, to one from a society that respects civil liberties and freedoms, to be an unwarranted intrusion upon one's being. The pervasive fear and anxiety of citizens in former Eastern Block nations with secret police and legions of informants have been well documented. Those circumstances stand in sharp contrast to the ideals of personal freedom that we cherish. When we refer to the excesses of the McCarthy era and to more recent programs that encourage and reward anonymous snitches, we usually do so in a pejorative manner.

Some searching questions must be asked before a nod is given to establishing a national customer name and address data base. To assess the validity of the need, questions such as those that follow must be posed and receive credible answers. To determine the validity of the purported need, one must clarify: What was the specific rationale for the recommendation to establish a national CNA data base? Was it based on the strength of an assumption or belief that data bases are intrinsically good? What specific need is it intended to satisfy - for whom? What will it make possible to do? What specifically will it be used for beyond what is done now, and exactly how will that improve security or law enforcement?

If answers to the foregoing questions pass muster, one must then ascertain the merits of proceeding. The following questions are appropriate: Who will use the data base? How will it be used? How often will it be used for each purpose? What will it cost and what payout is it expected to provide? In this latter regard, the assessment of cost must encompass what will be needed to develop, to implement, to load data, to operate, to maintain, and to upgrade and keep the data base current and synchronized with evolving technology. Only if all these are reasonably estimated can one credibly demonstrate the expected efficacy and benefit/cost value of a new national data base. One must still examine the opportunity cost involved to assess whether there might be better or more deserving uses of resources.

Even if a rigorous front-end assessment shows favourable results, a number of practical administrative considerations remain to be resolved. Decisions will be needed to clarify: who will specify the system requirements, who will specify the acceptance criteria, who will design it, who will oversee the development, who will be responsible for performance testing and acceptance, who will feed it data, who will manage it, who will be allowed to access the data, and lastly, who will pay for it. There will also be a need to develop protocols governing the operation and use of the data base and appropriate provisions to assure that civil liberties and freedoms are fully respected. Unless both a thorough need assessment and a robust feasibility study demonstrate that a national CNA data base is needed, the recommendation should be set aside.



## CONCLUSION

It is unquestionably important to ensure that authorities have the necessary powers to protect Canadians from major crimes and terrorism. It is equally important to ensure that the exercise of those powers does not infringe upon, negate or deny Canadians the very rights and freedoms that constitute a vital, cherished and hard-won part of the quality of life in our society, which the proposed powers are intended to protect.

We stress the importance of exercising the utmost care to ensure that stringent conditions are articulated and inserted into whatever legislative instruments are prepared to grant increased lawful access powers to law enforcement and security authorities. The sponsoring departments must clarify what controls there will be to safeguard against inappropriate use.

They must specify what essential conditions must be met in order to invoke any new orders that might be inserted into the Criminal Code or other legislation.

They must clarify what measures or procedures will have to be followed and satisfied to respect and maintain civil liberties and rights conferred by the Canadian Charter of Rights and Freedoms.

These will serve as safeguards against including provisions that facilitate unintended negative consequences in the exercise of any new lawful access powers that impact on law-abiding Canadians.

The Civil Liberties Association, National Capital Region would be willing to participate in reviews of any proposed draft legislation, amendments and regulations to assess civil liberties implications and identify ways to protect them.

Cloutier, Marie

---

From: [REDACTED]  
Sent: 2002 Dec 04 12:01 PM  
To: la-al@justice.gc.ca  
Subject: lawful access

s.19(1)

This lawful access proposal is crazy.  
Just what we Canadians need, to become the next USA.  
I guess it'll be time to stop using the internet if this ever becomes passed.  
I myself love privacy, i am law abiding, but i do NOT want my actions logged by anyone.  
Dont let our country become what George W Bush wants it to become. :(

[REDACTED]

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Dec 05 3:22 PM  
**To:** la-al@justice.gc.ca; liaison@justice.gc.ca  
**Subject:** Consultation and Outreach -- amendments to the Criminal Code dealing with the interception and search-and-seizure provisions

Sir/Madam,

I write this email in response to your "Consultation and Outreach" web page [http://canada.justice.gc.ca/en/cons/la\\_al/d.html](http://canada.justice.gc.ca/en/cons/la_al/d.html) where you consider Several amendments to the *Criminal Code* dealing with the interception and search-and-seizure provisions.

My background comprises: 20 years in the IT business and government of including experience as the second ISP in Ottawa, first private ISP in Frankfurt, and work in internet café.

Without getting into lengthy dissertations, I am strongly opposed to the government, laws and courts to compel ISPs to:

- a. Keep & collect client personal information (name, address, SIN, Ids, etc)
- b. Keep & collect logs before court orders are issued
- c. Keep & collect logs after court orders are issued without fair financial compensation
- d. Keep & collect transactions (e.g., email contents, chat sessions) before court orders are issued
- e. Keep & collect transactions (e.g., email contents, chat sessions) after court orders are issued without fair financial compensation
- f. Assist law-enforcement agencies without fair financial compensation

I believe that when determining "fair financial compensation" to which I eluded above, at least the following should be taken into account:

- a. The cost (salaries, contracts, benefits, etc) of the ISP people doing and managing the work (that the law enforcement agencies require) as well as setting up systems to enable such work
- b. Opportunity cost of not being able to use the services of these people on profitable ventures ... i.e., the hourly rate should be increased to match their normal charge-out rate to clients, and if not applicable, perhaps increase the amount by something reasonable like 50%
- c. Additional hardware, software, licences ... capital expenditure as well as on-going expenditure to keep these systems in operation
- d. Real-state /space costs and if required relocation costs to other offices
- e. The cost of possible loss of business if the word gets out that the ISP is giving up (too freely) personal/client information

[REDACTED] s.19(1)

Komokoa Corporation : [www.komokoa.com](http://www.komokoa.com)

Tel: +1 613 860-7878 [REDACTED]

**A Government-On-Line supplier**

---

The information contained in this email is private, privileged, confidential and copyright. If you received this email in error, please advise me immediately and delete it permanently from your computer. Interception of this email is a criminal offence as stipulated by section VI of the Criminal Code. Dissemination, distribution, copying, or use of this email or the information herein by other than the intended recipient is prohibited and protected by the Copyright Act and Privacy Act.

---

Cloutier, Marie

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 07 4:29 AM  
To: la-al@justice.gc.ca  
Cc: [REDACTED]  
Subject: 'Lawful Access' : Unlawful, Unconstitutional, Extraterritorial.

I am firmly against this idea, this EU export and the so-called Canadian revision of which, whose ambiguity lends suspect to insidiousness or incompetence.

And shame on the Justice Ministry who 'snack this under the table'. Such a significant ammendment of the 'Charter of Rights & Freedoms' surely deserves more than virtual obscurity and backdoor legislation. It requieres discussion, it requieres public participation, it requieres -detail- and, this perhaps may strike 'you' (whichever minion in the Justice Dept. reads this, I know no-one of influence will - but rhetorically I'm speaking to the Minister) as a strange notion, but also COST PROJECTIONS (!) Thus, I submit to you that only after you have a more detailed outline, can -constitutional- public input be provided. This consultation strikes me as farcical, feel free to correct me, but I am inclined to believe the consultation date has been extended either because you have'nt reached the 50-or-so responses quote, or that input thus far has been accutely against your extra-legalistic leap.

Let me thematically highlight the economic as well as libertarian drawbacks to this not-so-well thought-out proposal.

-----  
Immense costs passed directly to the Taxpayers:  
-----

This is my immediate concern (though it is not as more important than warrant-less search&seizure unconstititional precedence that would be set by the proposal) as I am law abiding. Having my isp rate double is certainly a real concern when it comes to -ANY- expenditure ventures of any sort whatsoever taken by any Ministry whatsoever in this government. I hope I'm clear on that point, and I would have hoped that after a 2 million projected (it was -projected- better than the vague & uncommitting proposal in question with virtually NO cost projection!) gun registration turns 500-fold, I think my suspicions, my right to be skeptical, is well arranted. This proposal will cause immense saturation; it will entail the need for a mmamoth expansion in hardware for the ISPs (the S stands for service, not SPY) which will the consumer will have to withstand. Canadian internet infrastructure is not up to par with the current members of the EU (except perhaps the U.K.), and the result will be immense saturation. The irony is that even if I accepted the need for the LA changes I would still claim that existing resources are sufficient ti facilitate it. The retention at ISPs in regards to users online activities are enough, there is no need to store a whole history of suspected person/s, what is available at the ISPs right now is enough to collect evidence and then & only then conduct an investigation. Thus the whol LA / EU approach is one of unfathomable wastefulness. I was unhappy when my ISP raised the price from \$50 to \$55, I will be extremely unhappy when it reaches the \$100 mark, and yet I fear worse from these government Ministry, though hopefully, -hopefully- it will not be 500-fold ; 500-fold of what(?), is a very pointed question that perhaps the advocates of the EU's LA should revisit (and by revist I mean 'visit').

-----  
Lawful Access, an Orwelian first step:  
-----

Tyranny & totalitarianism usually do not occur in one single stroke. Often there are 'steps' which facilitate these. By making one medium not subject to the still-soverign Canadian constitution, the stairway to lead to disaster is one step closer. Telephone will be next in 5 years, maybe 10 years; in 20 years the mail, and soon enough we will be there. But no matter who will be in power then, the historical responsibility, the moral responsibility will be on your shoulders; and your legacy will be forever

tainted. Canada should be making its own laws, and those laws which are de jure extraterritorial and de facto unconstitutional MUST be held to far closer scrutiny. There must be public participation, a "well-balanced" commission, and much, much more 'planning, testing, & objective-setting'. I feel almost odd seemingly lecturing to the -experts' about sound public policy formulation & planning, but then I think about that \$2 million = \$1 Billion gun registration, and suddenly it seems quite appropriate.

---

Conclusion: Lawful Access is Unlawful, Consultation Highly Insufficient

---

With this pseudo-consultative period; the level of exposure given to LA ; the extremely vague planning & cost prediction; the inevitable sizable costs involved & increased saturation; the extreme discrepancy between goals sought and the means to achieve these, and the lack of technical understanding on the part of LA/EU-law-revising policy makers; the extraterritorial infringement of sovereignty where it matters most - the constitution; the anti-privacy precedence and Orwellian first step, with all these either insidious or incompetent (my right to freely say just that is fast-dwindling, not incidentally) shortcoming, mean that the Justice Ministry has lost credibility on this issue, arguably (therefore) in general. I have no faith in the Justice Ministry. If there is a hope, enough public knowledge of this unconstitutional initiative will cause a public outcry (regretably, likely after the fact), and in spite of the Ministry's attempt to keep the whole thing 'quiet' and away from the public's ear, when the programme is actually implemented, it will take notice. Then one could hope that the Canadian Supreme Court (appointed by the same government, yes, but must still maintain a perception of impartiality, especially in regards to issues close to the public's eye, which this will be) will strike this proposal down for the blatant extra-legalism that is its nature, basically saying: if you want to enact is as a legislation, you need to change the constitution -first- .

Sincerely,

 s.19(1)

---

Tired of spam? Get advanced junk mail protection with MSN 8.  
<http://join.msn.com/?page=features/junkmail>

Pierlot, Paul

---

From: [REDACTED] s.19(1)  
Sent: 2002 Dec 08 7:01 PM  
To: la-al@justice.gc.ca  
Subject: Opinions on Lawful access

**POWER CURRUPTS. ABSOLUTE POWER, CURRUPTS ABSOLUTELY.**

Now, according to whoever made this proposed legislation up; **The government has justified its proposals by saying that Canada has to adapt the Criminal Code before it can ratify the Convention on Cyber-Crime, which Ottawa signed last November as a non-voting observer to the Council of Europe. The paper points to the difference between Canada and "several" other countries, which have already updated legislation to give security authorities "lawful access capabilities."**

But think of this. Why would Canada, a proudly sovereign nation be so concerned to implement the dictates of an organization in which it DOESN'T EVEN HAVE VOTING RIGHTS? This isn't the reason folks IT'S THE EXCUSE!!!!

I recall a while back, the Communication Security Establishment (CSE) in Ottawa wanted to be able to open every email coming into to country. The excuse? Get this!!! They say they want to protect Canadian business and consumers from viruses that come in email attachment!!!! Nice try boys and girls, but you'll have to come up with something better than this Load-Of-Crap to convince me that it's in me interest to let them read my love letters from my mistress overseas.

For those of you who like to swallow the hook, line, and sinker, ask yourself this: What can the CSE do, that an up to date copy of Norton or McAfee antivirus software can't do? As for Canadian business networks; There is literally tonnes of hardware and software out there to prevent virus and hacker attacks. Any business that in this day and age doesn't make use of this stuff, deserves to have their corporate network hacked into and screwed up.

Another thing I couldn't help but notice in this proposal: **The Canadian Association of Chiefs of Police has made recommendations...including the establishment of a national database. The implementation of such a database would presuppose that service providers are compelled to provide accurate and current information.**

Which Luddite police chief came up with this dumb idea? Moreover, considering that it's now the official request of the association as a whole, (I assume) that would mean it has the backing of the majority of it's members. Now let's think about this. We're talking about half of all households in Canada having internet access. Of what use would a list like this be to law-enforcement when almost half of all Canadians are on it? That would be like wanting a list of people who know how to use a telephone. And besides, the city is dotted with Internet cafes for those who don't have computers or Internet access. Has anyone seen the new Sympatico Internet booths downtown? The princely sum of \$2 gets you 10 minutes of serf time. Just enough time for a foreign business traveler to send an email update to the head office back home, or for a Qaeda operative to let Osama know how the planned CN Tower bombing is coming along. What will a list of Canadian Internet users do for this? Nothing!

I recall back in the good old days of the Cold War, The late 80's to be exact, I was on an Aeroflot flight from Moscow to Kingston Jamaica. I was beside a Jamaican student who was studying in the U.S.S.R. on scholarship. Did I mention it was a 18 hour flight with 2 refueling stops in Shannon, Ireland and Havana Cuba? No in-flight movies, magazines or booze? And you thought Tango and Air Transat was bad. Anyway, I was asking him what life was like behind the Iron Curtain, and one of the things he mentioned, was that anyone in the Soviet Union wanted to own a PC, had to get a license from the government. Just like how we have to have a FAC license to own a handgun. Now I don't know if post-communist Russia still has this stipulation, but isn't this pretty much what our Luddite police chiefs want? For us to have a license to use the Internet?

Good God!!!! I thought communism was dead and discredited. And these dinosaur police chiefs of Canada are trying to bring it back!!!!

**As for the police chiefs, did it ever occur to them that one day, they will actually retire and no longer have Peace-Officer status? That they will be among the very ones being spied on with the help of the very same legislation they were clamoring for?**

**Also, check this (nonsense) out: the type of criminals associated with some of these crimes is evolving. In telemarketing, for example, aliases are frequently used and there is a growing link between criminal elements associated with this kind of activity and threats to the security of Canadians.**

On the interception of email; Part VI of the *Criminal Code* creates...a scheme for obtaining judicial authorization to intercept such communications. The requirements for intercepting a "private communication" are more onerous than those required to obtain a search warrant to seize documents or records. Section 183, in Part VI of the *Criminal Code*, defines the expression "private communication" to cover any *oral* communication, or any telecommunication made under circumstances creating a reasonable expectation of privacy. This appears to suggest that, once a communication is put in writing, it can no longer be considered a "private communication" for the purpose of the interception of communications provisions of the *Criminal Code*.

**In fact, some courts have held that a tape-recorded message, like a written letter, did not fall within the definition of "private communication" because it was not reasonable for a person sending such a tape (or letter) to expect that it would remain completely private. As it was a permanent record of its contents, it could easily come into the hands of a third party. Following this line of reasoning, one could argue that e-mail communications, as they are in writing, would not come within the "private communication" definition. Therefore, these written records could be obtained by a search warrant.**

**However, some cases dealing with e-mails in Canada have taken the position that they are to be considered "private communications." For example, a judge in Alberta recently held that judicial authorization under Part VI was required to intercept e-mails since there was a reasonable expectation of privacy on the part of those sending and receiving them.**

**These decisions, along with the definition of "private communication," create some confusion as to whether an e-mail should be seized or intercepted.**

**Brrrrrrrrrrrrr.....this one gives me the chills. I used to work as a technician for Cable and Wireless Jamaica, And with the greatest of ease, used to be able to listen to "private, oral" conversations of subscribers with use of a tool called a "butt-in", which every telco tech needs in order to do his job....and that without them even knowing! Yet callers (rightfully) expect their calls to be done without me getting off on their phone-sex talk.**

Now some will say that the telco has rules against me doing that....and right they are. Guess what. Your friendly neighborhood postie also has rules against opening your mail with out your consent. If you weren't expecting that written communication to be private, why would you put it in an envelope and seal it? Obviously, Mastercard and Visa also expects their correspondence to be private too. Else they wouldn't be sending your credit card to you via mail, would they now?



Another thing. Since they want to get at my ordinary emails without warrant since I don't "expect any privacy", what if I encrypt them? Surely they can't argue in court that I'm not expecting privacy since I made it impossible for anyone to simply read my email without jumping through hoops. This isn't exactly an open postcard I'm mailing here.

This whole argument of theirs is rubbish, total rubbish.

Some will chime in; "since 9/11, we now live in different world where we simply can't expect as much freedom anymore". But isn't this the very way Islamic extremists want us to live? Are we not actually imposing our own version of Wahhabism on our selves at the extremists behest? If we so readily give up our rights, freedoms, and liberties in the name of fighting terrorism, then in fact, we have already lost the war. Yes, there is an element of risk along with freedom. It has **always** been that way before the World Trade Center towers came crashing down. It **will** always be that way, even after Osama and company are long dead.

In a recent U.S. Supreme Court case of *Watchtower Bible and Tract Society of New York, Inc., et al. V. Village of Stratton et al*, Justice Antonin Scalia observed; **"We can all stipulate that the safest societies in the world are totalitarian dictatorships. There's very little crime. It's a common phenomenon, and one of the costs of liberty is to some extent a higher risk of unlawful activity, and the question is whether what this is directed at stops enough unlawful activity to be worth the cost..."**

Yeah, yeah, I know. The U.S. Supreme Court has no jurisdiction in Canada. Nevertheless, Justice Scalia's comments are universal in nature and are worth reflecting on.

In general, I fear that at the current rate with which citizens privacy, sanctity of the abode, freedom of the body, erosion to freedom of personal expression and especially, the erosion of individual Canadian's expectation of privacy, along with the infantilisation of Western adults, Canada will be a full blown police state within 20 to 30 years. If we even still do have something resembling elections, they will merely be a token display without the essence thereof, such as is now practiced in Cuba, Iraq, Iran, and Hong Kong. Personally, I don't know of too many Canadians interested in migrating to these places. In fact we have large numbers of new Canadians fleeing from these very places.

s.19(1)



Pierlot, Paul

From: [REDACTED] s.19(1)  
Sent: 2002 Dec 09 12:14 AM  
To: la-al@justice.gc.ca  
Subject: Lawful Access Consultation Submission  
9 December 2002

EMAIL TO: la-al@justice.gc.ca  
Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor,  
284 Wellington Street  
Ottawa, ON K1A 0H8  
Canada

Gentlemen:

Re: "Lawful Access" Proposals - Comment Submitted Herein

As the deadline for submission of public comments on the "Lawful Access" proposals has been extended to 16 December 2002, the following comments are submitted at this time. This submission is posted online at <http://members.execulink.com/~kerisler/acsub.htm> in HTML and in Adobe Acrobat PDF format:

### ***"Lawful Access" Proposals Flawed***

The Canadian government proposals re what it terms "Lawful Access" sound superficially reasonable in principle. These proposals are outlined in the *Lawful Access Consultation Document* as posted in Adobe Acrobat and in HTML format at: [http://www.canada.justice.gc.ca/en/cons/la\\_al/](http://www.canada.justice.gc.ca/en/cons/la_al/).

The document asserts that:

*The public policy objectives of this process are to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada.*

The document seems to imply that in order to fight "cybercrime," and to meet a claimed treaty obligation, enforcement and spy authorities must be assigned a similar power to intercept communication, with appropriate authorization, as now exists regarding telephone records and other pre-Internet communications.

The proposals are over-reaching in that the Internet and other new communications systems are not simple structures with direct parallels to the earlier analog telephone technology.

The fault lies in a failure to appreciate that the Internet as well as service providers who would be required to log citizen activity are not simply connective mechanisms that keep logs. They are in practice a collective services mechanism that accepts, stores, and offers data from telephone calls, broadcast sources, print sources, citizen sources, and other mechanisms. Logged records of Internet activity are by nature highly revealing of the user's private life.

The consultation document also asserts that *"There is currently no legislative mechanism in Canada that can be used to compel service providers to develop or deploy systems providing interception capability, even if a legal authorization is obtained by law enforcement or national security officials to intercept the communications of a specific target."*

The assertion begs the question as to why there should necessarily exist such a mechanism. We could argue that people meet commonly in malls and other public places and yet we would not seriously entertain the assertion that some sort of "intercept" system need be in place at malls and on public streets to facilitate listening in on

citizens.

It also presumes that the referenced "cybercrime" treaty truly mandates such a requirement at all. The neutral observer may wonder whether the cybercrime treaty in context is more a rhetorical prop than a guiding justification.

### ***Internet Logs Reveal More than Telephone Records***

Once we decide to log a person's Internet connectivity we are not merely creating the equivalent of a telephone call log, to draw a parallel with the process whereby telephone companies-creatures of the previous pre-Internet era-routinely log numbers called for all customers.

When we create a parallel kind of log for the Internet we are creating a record of a person's life that goes far beyond the mere equivalent of telephone number records. The hyperlink record, after all, normally specifies not just web pages, but may capture picture file names, document file names, audio and print information file names, and more.

Consider these examples.

This hyperlink displays a news story on so-called "Lawful Access" proposals:  
[http://news.com.com/2100-1023-955595.html?tag=fd\\_top](http://news.com.com/2100-1023-955595.html?tag=fd_top)

This hyperlink is to an Adobe Acrobat PDF-format file:  
<http://members.execulink.com/~kerisler/downloads/msi/RDRAGMSI.exe>

This hyperlink is to an Advanced Photo System (APS) photograph of anonymous graffiti:  
[http://members.execulink.com/~kerisler/images/LPS\\_Bridge\\_Graffiti.jpg](http://members.execulink.com/~kerisler/images/LPS_Bridge_Graffiti.jpg)

The above hyperlinks, were they part of a person's web browsing record, could tell us something about the individual beyond what a simple pre-Internet log of dialed telephone numbers could tell us.

The first hyperlink suggests an interest in civil liberty issues; the second is to an article (albeit password-locked) which details how to keep one's software properly updated to assure proper PC functionality; the final hyperlink is to a photo-and the adage that does apply here is that a photo is worth a thousand words. A browsed-to photo's content might reveal a great deal about the person-but not reveal anything illegal at all.

But in *all* of the above examples, *all* of the hyperlinks listed above suggest more information about the person who browsers to them than a superficial record of a telephone number they might have dialed pre-Internet would reveal.

The fact that the "Lawful Access" proposals talk about more than the Internet, and even reference database possibilities, extends the threat proposed by Internet/services logging even further than simple web browsing.

Much content intended for cellular telephones, as well as sent from such phones, may now also be transferred via the Internet. Logging these data transactions as web activity would in fact *extend* the eavesdropping rights of the authorities, as it would mean that lots of cell phone activity (SMS text messages, browsing from cell phones) would also be captured in Internet logs.

Moreover, Canada's official federal Privacy Commissioner George Radwanski has noted similar concerns in stating that:

*Although the proposals outlined in the consultation paper purport to adapt or maintain law enforcement access to communications data, it is clear that this new instrument will go far beyond accessing a simple record of numbers called or received to include very intimate details and a much larger profile of our activities, thoughts, preferences, and lifestyle.*<sup>(1)</sup>

### ***"Lawful Access" Elevates Some Eavesdropping Entitlements***

So the "Lawful Access" proposal is not in itself neutral or merely extending to cyber realms what already exists; with respect to cellular text transmission and web browsing, the proposals would actually broaden the eavesdropping rights of enforcement bodies.

### ***"Lawful Access" Parallel with Old Tech Invalid***

The foregoing does suggest that the inferred parallel made by the "Lawful Access" proposals between pre-Internet access entitlements and Internet/services access needs is significantly over-reaching and therefore invalid.

If we say that a parallel between previous technologies and new technologies must be established to allow law enforcement an equal chance to police new technology realms, we must fairly and reasonably apply an effects-grounded test for such needs, rather than the crude pseudo-parallelism that is oddly and uncomfortably applied from the get-go in the euphemistic phrasing "Lawful Access."

If we take telephone records as a log example, we can clearly see the need for cybercrime log limits. When telephone companies retained call logs in the past-such dialed-number logs being available to law enforcement with proper authorizations-such records did not relate to or indicate content directly or indirectly.

A record that says Joe Smith called (555) 672-2372 on 21 November 2002 at 9:00 A.M. tells us potentially the location and account holder name of the number called, but in itself imparts no information as to content. It does not even tell us who picked up the telephone that was dialed!

Presumably honest law enforcement personnel would seek proper court authorization for any desired telephone wiretap that might, with the benefit of such authorization, monitor any content of calls. But until then the important and essential reality is that no content is revealed by the pre-wiretap log itself.

### ***Genuine Parallel Entitlement Much More Limited***

We should apply a similar parallel in defining what an ISP may log. Taking the valid old technology parallel, it is reasonable that ISPs should not be required by law, and indeed should be expressly prohibited from logging, any hyperlinks or other records that might reveal contents.

A reasonable limitation is that an ISP should morally and legally only log times of log-on and log-off, and possibly the base URLs of sites visited, but no hyperlinks to files, pages or pictures beyond single top-level web page links. And such hyperlinks to main web site home pages should be legally logged only in so far as they may be needed to meter online charges or other customer uses for the purposes of maintaining a customer-business relationship.

At bottom we do not have telephone companies log called numbers for the purpose of facilitating spying on citizens when police or other agencies feel the urge to do so. And yet the tone and tenor of the "Lawful Access" proposals, starting with the rhetorically loaded straw man of the term "Lawful Access" itself, struggles hard to convince us, quite weakly overall, that this is the case.

We should not enshrine any greater entitlements regarding logging of "cyber" services, or in other future communication services. Limitations on logging as suggested above would move toward a more reasonable citizen-respecting model for the online and new communications services realms.

Further, there should be no weakened standards of proof used in the process of justifying electronic eavesdropping on the Internet and in any other new communications realms. The "Lawful Access" proposals seem to suggest weaker standards than in the past, and that is unacceptable.

### ***Limitations Needed Even When Spying Properly Authorized***

We must also be concerned beyond the point where state enforcement and spying authorities gain by warrant or whatever method the silent right to spy on the end user.

Logically, the obtaining of whatever warrants or other (unacceptable) lesser permissions may be required for such spying should not holus bolus permit the sudden use of file-, page-, photo-, and/or document-specific web link records unconditionally, but should be highly specific authorization-wise, even post-warrant, about exactly which kinds of links may be tracked actively once warrants have been obtained.

Further, such permissions to track the user, if enacted at all, should be far more strictly regulated than previous permissions such as those allowing phone tracking, precisely because the data that will be captured will certainly be greatly revealing of the targeted citizen's private life, as noted previously.

Thanks for the opportunity to comment on the "Lawful Access" proposals.

Sincerely,

London, ON Canada

s.19(1)

Please ignore unreadable formatting & digital security  
attachments used only by up-to-date email programs

Ref: Lawful Access Consultation Submission.doc

---

<sup>[1]</sup> 25 November 2002 letter to the Honourable Martin Cauchon, Minister of Justice and the Attorney General of Canada, the Honourable Wayne Easter, Solicitor General of Canada, and the Honourable Allan Rock, Minister of Industry.



s.19(1)

JOURNALISM/COMMUNICATIONS/PHOTOGRAPHY

Telephone: (519) 851-1323

Fax: (630) 214-5568

9 December 2002

Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor,  
284 Wellington Street  
Ottawa, ON K1A 0H8  
Canada

Gentlemen:

Re: "Lawful Access" Proposals – Comment Submitted Herein

As the deadline for submission of public comments on the "Lawful Access" proposals has been extended to 16 December 2002, the following comments are submitted at this time. This submission is posted online at <http://members.execulink.com/~kerisler/acsub.htm> in HTML and in Adobe Acrobat PDF format:

### ***"Lawful Access" Proposals Flawed***

The Canadian government proposals re what it terms "Lawful Access" sound superficially reasonable in principle. These proposals are outlined in the *Lawful Access Consultation Document* as posted in Adobe Acrobat and in HTML format at: [http://www.canada.justice.gc.ca/en/cons/la\\_al/](http://www.canada.justice.gc.ca/en/cons/la_al/).

The document asserts that:

*The public policy objectives of this process are to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada.*

The document seems to imply that in order to fight "cybercrime," and to meet a claimed treaty obligation, enforcement and spy authorities must be assigned a similar power to intercept communication, with appropriate authorization, as now exists regarding telephone records and other pre-Internet communications.

The proposals are over-reaching in that the Internet and other new communications systems are not simple structures with direct parallels to the earlier analog telephone technology.

The fault lies in a failure to appreciate that the Internet as well as service providers who would be required to log citizen activity are not simply connective mechanisms that keep logs. They are in practice a collective services mechanism that accepts, stores, and offers data from telephone calls, broadcast sources, print sources, citizen sources, and other mechanisms. Logged records of Internet activity are by nature highly revealing of the user's private life.

The consultation document also asserts that *"There is currently no legislative mechanism in Canada that can be used to compel service providers to develop or deploy systems providing interception capability, even if a legal authorization is obtained by law enforcement or national security officials to intercept the communications of a specific target."*

The assertion begs the question as to why there should necessarily exist such a mechanism. We could argue that people meet commonly in malls and other public places and yet we would not seriously entertain the assertion that some sort of "intercept" system need be in place at malls and on public streets to facilitate listening in on citizens.

It also presumes that the referenced "cybercrime" treaty truly mandates such a requirement at all. The neutral observer may wonder whether the cybercrime treaty in context is more a rhetorical prop than a guiding justification.

### ***Internet Logs Reveal More than Telephone Records***

Once we decide to log a person's Internet connectivity we are not merely creating the equivalent of a telephone call log, to draw a parallel with the process whereby telephone companies—creatures of the previous pre-Internet era—routinely log numbers called for all customers.

When we create a parallel kind of log for the Internet we are creating a record of a person's life that goes far beyond the mere equivalent of telephone number records. The hyperlink record, after all, normally specifies not just web pages, but may capture picture file names, document file names, audio and print information file names, and more.

Consider these examples.

This hyperlink displays a news story on so-called "Lawful Access" proposals:

[http://news.com.com/2100-1023-955595.html?tag=fd\\_top](http://news.com.com/2100-1023-955595.html?tag=fd_top)

This hyperlink is to an Adobe Acrobat PDF-format file:

<http://members.execulink.com/~kerisler/downloads/msi/RDRAGMSI.exe>

This hyperlink is to an Advanced Photo System (APS) photograph of anonymous graffiti:

[http://members.execulink.com/~kerisler/images/LPS\\_Bridge\\_Graffiti.jpg](http://members.execulink.com/~kerisler/images/LPS_Bridge_Graffiti.jpg)

The above hyperlinks, were they part of a person's web browsing record, could tell us something about the individual beyond what a simple pre-Internet log of dialed telephone numbers could tell us.

The first hyperlink suggests an interest in civil liberty issues; the second is to an article (albeit password-locked) which details how to keep one's software properly updated to assure proper PC functionality; the final

hyperlink is to a photo—and the adage that does apply here is that a photo is worth a thousand words. A browsed-to photo's content might reveal a great deal about the person—but not reveal anything illegal at all.

But in *all* of the above examples, *all* of the hyperlinks listed above suggest more information about the person who browsers to them than a superficial record of a telephone number they might have dialed pre-Internet would reveal.

The fact that the "Lawful Access" proposals talk about more than the Internet, and even reference database possibilities, extends the threat proposed by Internet/services logging even further than simple web browsing.

Much content intended for cellular telephones, as well as sent from such phones, may now also be transferred via the Internet. Logging these data transactions as web activity would in fact *extend* the eavesdropping rights of the authorities, as it would mean that lots of cell phone activity (SMS text messages, browsing from cell phones) would also be captured in Internet logs.

Moreover, Canada's official federal Privacy Commissioner George Radwanski has noted similar concerns in stating that:

*Although the proposals outlined in the consultation paper purport to adapt or maintain law enforcement access to communications data, it is clear that this new instrument will go far beyond accessing a simple record of numbers called or received to include very intimate details and a much larger profile of our activities, thoughts, preferences, and lifestyle.<sup>1</sup>*

### **"Lawful Access" Elevates Some Eavesdropping Entitlements**

So the "Lawful Access" proposal is not in itself neutral or merely extending to cyber realms what already exists; with respect to cellular text transmission and web browsing, the proposals would actually broaden the eavesdropping rights of enforcement bodies.

### **"Lawful Access" Parallel with Old Tech Invalid**

The foregoing does suggest that the inferred parallel made by the "Lawful Access" proposals between pre-Internet access entitlements and Internet/services access needs is significantly over-reaching and therefore invalid.

If we say that a parallel between previous technologies and new technologies must be established to allow law enforcement an equal chance to police new technology realms, we must fairly and reasonably apply an effects-grounded test for such needs, rather than the crude pseudo-parallelism that is oddly and uncomfortably applied from the get-go in the euphemistic phrasing "Lawful Access."

---

<sup>1</sup> 25 November 2002 letter to the Honourable Martin Cauchon, Minister of Justice and the Attorney General of Canada, the Honourable Wayne Easter, Solicitor General of Canada, and the Honourable Allan Rock, Minister of Industry.



If we take telephone records as a log example, we can clearly see the need for cybercrime log limits. When telephone companies retained call logs in the past—such dialed-number logs being available to law enforcement with proper authorizations—such records did not relate to or indicate content directly or indirectly.

A record that says Joe Smith called (555) 672-2372 on 21 November 2002 at 9:00 A.M. tells us potentially the location and account holder name of the number called, but in itself imparts no information as to content. It does not even tell us who picked up the telephone that was dialed!

Presumably honest law enforcement personnel would seek proper court authorization for any desired telephone wiretap that might, with the benefit of such authorization, monitor any content of calls. But until then the important and essential reality is that no content is revealed by the pre-wiretap log itself.

### ***Genuine Parallel Entitlement Much More Limited***

We should apply a similar parallel in defining what an ISP may log. Taking the valid old technology parallel, it is reasonable that ISPs should not be required by law, and indeed should be expressly prohibited from logging, any hyperlinks or other records that might reveal contents.

A reasonable limitation is that an ISP should morally and legally only log times of log-on and log-off, and possibly the base URLs of sites visited, but no hyperlinks to files, pages or pictures beyond single top-level web page links. And such hyperlinks to main web site home pages should be legally logged only in so far as they may be needed to meter online charges or other customer uses for the purposes of maintaining a customer-business relationship.

At bottom we do not have telephone companies log called numbers for the purpose of facilitating spying on citizens when police or other agencies feel the urge to do so. And yet the tone and tenor of the "Lawful Access" proposals, starting with the rhetorically loaded straw man of the term "Lawful Access" itself, struggles hard to convince us, quite weakly overall, that this is the case.

We should not enshrine any greater entitlements regarding logging of "cyber" services, or in other future communication services. Limitations on logging as suggested above would move toward a more reasonable citizen-respecting model for the online and new communications services realms.

Further, there should be no weakened standards of proof used in the process of justifying electronic eavesdropping on the Internet and in any other new communications realms. The "Lawful Access" proposals seem to suggest weaker standards than in the past, and that is unacceptable.

### ***Limitations Needed Even When Spying Properly Authorized***

We must also be concerned beyond the point where state enforcement and spying authorities gain by warrant or whatever method the silent right to spy on the end user.

Logically, the obtaining of whatever warrants or other (unacceptable) lesser permissions may be required for such spying should not holus bolus permit the sudden use of file-, page-, photo-, and/or document-specific web

link records unconditionally, but should be highly specific authorization-wise, even post-warrant, about exactly which kinds of links may be tracked actively once warrants have been obtained.

Further, such permissions to track the user, if enacted at all, should be far more strictly regulated than previous permissions such as those allowing phone tracking, precisely because the data that will be captured will certainly be greatly revealing of the targeted citizen's private life, as noted previously.

Thanks for the opportunity to comment on the "Lawful Access" proposals.

Sincerely,

s.19(1)



Ref: Lawful Access Consultation Submission.doc

Pierlot, Paul

---

From: [REDACTED] s.19(1)  
Sent: 2002 Dec 10 2:49 PM  
To: la-al@justice.gc.ca  
Cc: Yves Côté; Yvon Brunelle; Y. Brunelle; Yvon (1) Brunelle; Sider.Justine@ic.gc.ca  
Subject: Commentaires Accès légal



Commentaires  
02.12.16.doc

Bonjour,

Voici les commentaires de l'Association des Compagnies de Téléphone du Québec (ACTQ) au document de consultation publique sur l'accès légal.





s.19(1)

228, rue Petit-Bourg  
Repentigny (Québec) J6A 7C1  
Téléphone : (450) 582-0011  
Télécopieur : (450) 582-2101  
Courriel : [redacted]

Le 10 décembre 2002

Consultation sur l'Accès légal  
Section de la politique en matière de droit pénal  
284, rue Wellington  
5<sup>e</sup> étage  
Ottawa (Ontario) K1A 0H8

Madame, Monsieur,

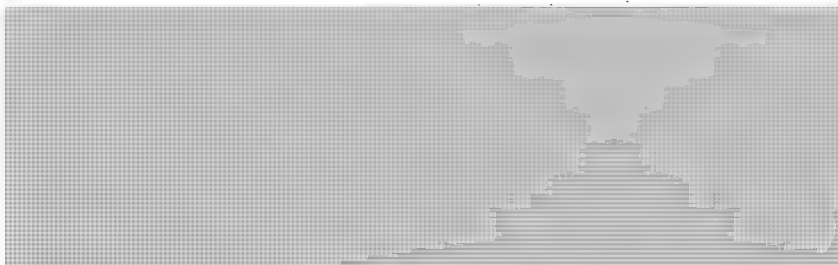
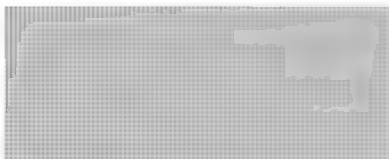
L'Association des Compagnies de Téléphone du Québec (ci-après appelée l'ACTQ) au nom de ses membres indiqués en annexe A, désire formuler ses commentaires suite à la présentation via conférence téléphonique le 3 décembre 2002, intitulée : « Consultation sur l'accès légal, Secteur des télécommunications, le 19 septembre 2002 ».

L'interception légale des communications et les procédures de perquisitions et saisies de données de façon autorisée par la Loi, les exigences relatives à l'infrastructure, la modification de certaines Lois fédérales, les méthodes pour obtenir le nom et l'adresse d'un abonné (NAA) et l'identité du fournisseur de services locaux (IFSL), sont d'autant d'éléments qui sont actuellement à l'étude par vos divers groupes internes.

Conséquemment, l'ACTQ ne possédant que peu de détails à ce sujet, ne peut formuler de commentaires précis dans ce dossier. Cependant compte tenu que la totalité de ses membres sont des entreprises de petite taille, l'ACTQ recommande que les nouvelles Lois proposées tiennent compte de ce fait.

Aussi, tel que préconisé dans votre étude préliminaire, ces Lois devraient être applicables seulement lors d'achat par ces entreprises, de nouveaux commutateurs ou lors de la mise en opération de nouveaux services (logiciels). De plus, tout nouveau service obligatoire et exigible par ces Lois, nécessitant des investissements accrus pour ces petites entreprises, devrait être compensé à 100% ou faire l'objet d'exemptions.

Finalement, l'ACTQ demande d'être consultée avant la présentation de toute Loi pertinente à l'Accès légal, à la Chambre des Communes. N'hésitez pas à communiquer avec le soussigné pour tout renseignement additionnel.





Information and Privacy  
Commissioner/Ontario  
Commissaire à l'information  
et à la protection de la vie privée/Ontario

D02-0572  
E02  
15-00-27

December 10, 2002

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, Ontario  
K1A 0H8

VIA FACSIMILE

Attention: The Honourable Martin Cauchon  
Minister of Justice and the Attorney General of Canada

Dear Minister:

RE: Lawful Access Consultation Paper

I am writing in response to the "Lawful Access" proposals that have been put forward by the Minister of Justice and Attorney General of Canada, the Solicitor General of Canada and the Minister of Industry.

I support the views of my federal colleague, Mr. George Radwanski, the Privacy Commissioner of Canada, who has prepared a lengthy and detailed response to the Lawful Access consultation paper. While I have a number of concerns with the proposals, I shall restrict my comments to a few key issues.

From the outset let me state that, absent both a clear demonstration of why these broad measures are necessary, together with a strong plan for oversight and protection of civil rights, I cannot and do not support the proposed legislative initiatives as currently described.

My concerns for the protection of privacy from unnecessary erosion extend beyond the "Lawful Access" proposals outlined in the consultation paper. In the past year, Canadians have been faced with an array of legislation that has been unprecedented in the scope and breadth of its capacity to diminish the privacy of individuals. The legislative juggernaut began with the omnibus Bill 36 that became the *Anti-terrorism Act*, followed by the equally vast omnibus Bill 42. Later, Bill 42 became Bills 44 and 55 (now C-17). Next came the privacy-invasive provisions of the Canada Customs and Revenue Agency's traveller-surveillance database. All of this legislation, together with ancillary regulations, has been introduced in pieces without a clearly articulated context and with very little discussion. The consultations, when provided, are narrowly defined and do not demonstrate a clear link between identified concerns and tailored solutions which can be supported and justified in a society such as ours.

Turning specifically to the Lawful Access Report (the "Report"), I am concerned that a number of provisions pose significant negative privacy implications.

.../2



80 Bloor Street West,  
Suite 1700,  
Toronto, Ontario  
M5S 2V1

80, rue Bloor ouest  
Bureau 1700  
Toronto (Ontario)  
M5S 2V1

INFORMATION & PRIVACY CUMM.

416-326-3333  
1-800-387-0073  
Fax/Télé: 416-325-9195  
TTY: 416-325-7539  
http://www.ontario.ca 000225

10-2002 14:24

## Limited Oversight

The Report demands high levels of citizen trust towards the law enforcement and intelligence communities. It argues for the need to narrow individual citizen's boundaries for informational self-determination, suggesting this will increase collective public security. The request for trust comes without parallel evidence of the need for this kind of legal change. I suggest that broad judicial or other oversight mechanisms be built into the lawful access proposal to ensure public accountability, transparency and scrutiny. This oversight body should require routine reporting on measures undertaken in the name of law enforcement and an accounting of the efficacy of these measures. This reporting requirement should enhance public confidence.

## Determination Test

Last year I suggested an approach to achieving both privacy and security. I recommended that a determination must first be made as to whether new powers being introduced were actually necessary, or whether a full deployment of existing investigative tools, already available to law enforcement and intelligence agencies, would suffice. If extended powers are indeed believed to be necessary, then we must ensure that they are used and deployed in a manner consistent with specific law enforcement objectives. The power to deploy new methods of surveillance must only be used to meet legitimate law enforcement goals. The information collected through these powers must only be used for identified law enforcement purposes and not for other purposes unrelated to public safety. Further, there is also a responsibility on the part of law enforcement officials, as counter-intuitive as it may sound, to protect the confidentiality of that information, particularly if it proves to have no relevance to law enforcement.

My colleague, the Privacy Commissioner of Canada, also proposed an excellent analytical and determinative test. I believe that these tests are now relevant more than ever.

## Old Standards Applied to New System

In viewing the impact and effect of new technologies, we cannot simply impose old standards of surveillance on new systems without recognizing that digital infrastructures complicate the application of dated analogue surveillance capabilities and legal rules. Wiretapping on an analogue telephone system is not comparable to the interception or monitoring of wireless communications or digital and Internet systems, which can provide more personal information and be more privacy invasive. We must re-think our approach rather than simply extending existing procedures to new technology.

There are also significant privacy and economic implications in developing the required surveillance infrastructure. While recognizing that interception capabilities are a necessary tool for law enforcement purposes, we would seek adequate safeguards to avoid any long-term data retention strategies and monitoring. If specific interception capabilities are mandated, there should also be parallel mandates regarding the access, use, disclosure, retention, security and disposal of data, together with effective oversight.

.../3

TOTAL P.04

- 3 -

Mandating that Internet Service Providers (ISPs) track all online activities of their clients, so that this information could potentially be used for evidentiary purposes, would require a massive investment in storage capacity for all ISPs. Many of them would face significant business repercussions and/or cause them to raise fees substantially, impeding the penetration of online services in our society. This could well result in industry consolidation that would have negative implications for privacy and free speech as well as the overall growth and development of the Internet as a communications medium. Furthermore, this massive aggregation of data will be of little use to law enforcement agencies unless they have the adequate resources to review and analyze the vast amounts of data that would be generated daily.

I continue to have grave concerns about the resulting massive surveillance initiative that has the potential to significantly diminish the privacy of all Canadians. While certain privacy-invasive measures may be necessary for anti-terrorism purposes, it is unacceptable to use the guise of anti-terrorism to develop broad-based law enforcement powers that routinely diminish the rights and freedoms that Canadians hold dear.

I urge you to reconsider the scope and direction of the lawful access provisions and urge you to address the important concerns identified by the Privacy Commissioner of Canada. Thank you for your consideration.

Sincerely yours,



s.19(1)

Ann Cavoukian, Ph.D.  
Commissioner

cc. The Honourable Wayne Easter, Solicitor General of Canada  
The Honourable Allan Rock, Minister of Industry  
Mr. George Radwanski, Privacy Commissioner of Canada  
Provincial/Territorial Privacy Commissioners and Ombudsmen

Office of the Information and Privacy Commissioner/Ontario  
Bureau du commissaire à l'information et à la protection de la vie privée/Ontario

FACSIMILE TRANSMISSION/TRANSMISSION PAR TÉLÉCOPIEUR

Date: December 10, 2002

To: THE HONOURABLE MARTIN CAUCHON  
Minister of Justice and Attorney General of Canada

Facsimile Number: (613) 995-0114

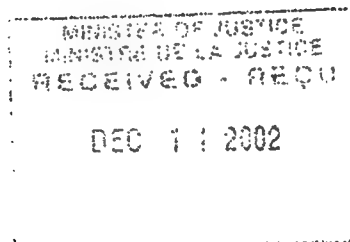
Telephone Number: (613) 995-7691

From: DR. ANN CAVOUKIAN, Commissioner  
Information and Privacy Commission/Ontario  
80 Bloor Street West, Suite 1700, Toronto, Ontario M5S 2V1

Telephone Number: (416) 326-3948

Facsimile Number: (416) 325-9195

Comments:



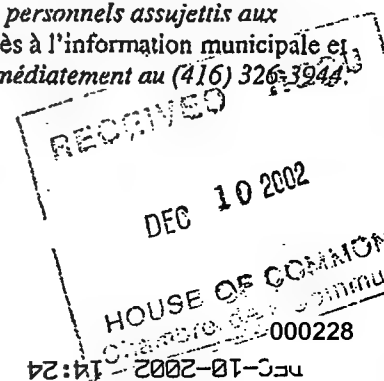
Number of pages including cover sheet: 4

The attached material is intended for the use of the individual or institution to which this telecopy is addressed and may not be distributed, copied or disclosed to other unauthorized persons. This material may contain confidential or personal information which may be subject to the provisions of the Freedom of Information and Protection of Privacy Act or the Municipal Freedom of Information and Protection of Privacy Act. If you receive this transmission in error, please notify us immediately by telephone at (416) 326-3333. Thank you for your co-operation and assistance.

*Les documents ci-joints sont destinés à l'usage exclusif de la personne ou de l'organisme destinataire et ne peuvent être copiés ni distribués ou divulgués à d'autres personnes. Ils peuvent contenir des renseignements confidentiels ou personnels assujettis aux dispositions de la Loi sur l'accès à l'information et la protection de la vie privée ou de la Loi sur l'accès à l'information municipale et la protection de la vie privée. Si vous avez reçu ces documents par erreur, veuillez nous téléphoner immédiatement au (416) 326-3944. Merci de votre collaboration.*



Information and Privacy  
Commissioner/Ontario  
Commissaire à l'information  
et à la protection de la vie privée/Ontario





**Ministerial Correspondence Unit / Unité de la Correspondence Ministérielle**  
**Routing Slip / Feuille de controle**

Letter/Lettre Date: 2002-12-10

**Author/  
Auteur:**

**Ann Cavoukian**

Commissioner  
Information and Privacy Commission  
80 Bloor Street West, Suite 1700  
Toronto ON  
M5S 2V1

**Document: 2002-025723**

**Doc Type/Type de Doc: D**

**File / Classer: 150027**  
**LAW - LAWFUL ACCESS**

*Reg*

**Referred To/Transmis a: MCUED2**

**Date: 2002-12-16**

**Due Date/Date d'échéance: 2003-01-16**

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

**Additional Comments / Remarques additionelles:**

**CC:**  
**CC:**

**CC:**  
**CC:**

**CC:**  
**CC:**

**CC:**  
**CC:**

**Closed / Fermer:**

**File Away / Classer:**

**Description of type / Description des types**

D: yellow docket / dossier jaune (draft response / projet de réponse)

A: further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

follow-up at your discretion / donner suite à votre discrétion

for your information (no action required) / à titre d'information (aucune mesure requise)



Royal Canadian Mounted Police  
Gendarmerie royale du Canada

Security Classification/Designation  
Classification/désignation sécuritaire

Unclassified

RCMP Police  
Special 'I' Section  
920 - 16th Ave. NE  
Calgary, Alberta  
T2E 1K9

Your File      Votre référence

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, Ontario

Our File      Notre référence

02 Dec 10

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official response from the RCMP Calgary, Alberta Special "I" Section, with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

Lawful access is an extremely important, and a very useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorist acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorized to intercept a communication or search and seize data.

We support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications technologies. We look forward to the opportunity to continue discussions on this issue as the lawful access legislative review progresses.

Sincerely,

  
W.D. Axley, S/Sgt.  
NCO I/C Calgary Special 'I' Section

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

Canada

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Dec 11 1:17 PM  
**To:** 'la-al@justice.gc.ca'  
**Subject:** Lawful Access Consultation Document Response

s.19(1)



Consultation Response

- Letter...

Please see attached letter. Signed original will follow in mail.

<<Consultation Response - Letterhead.doc>>



# Abbotsford Police Department

2838 Justice Way, Abbotsford, BC V2T 3P5 Phone (604) 859-5225 Fax (604) 859-4812

*"Protecting with Pride"*

*Chief Constable*

*Deputy Chief Constable*

December 11, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor - 284 Wellington Street  
Ottawa, ON K1A 0H8  
Canada

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Abbotsford Police Department with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Abbotsford Police Department agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief Constable  
Abbotsford Police Department

Cc: Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

*In partnership with the citizens of Abbotsford, we are dedicated to ensuring safety and security  
by enforcing the law, preventing crime and responding to community needs.*

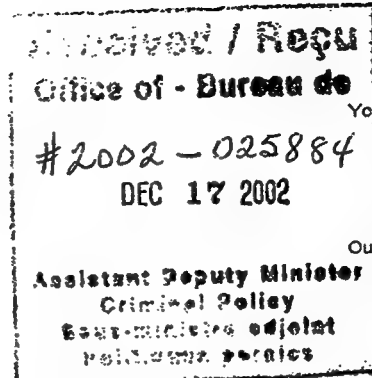
000232



Royal  
Canadian  
Mounted  
Police

Gendarmerie  
royale  
du  
Canada

Security Classification / Designation  
Classification / Désignation sécuritaire



Your file

Votre référence

Our file

Notre référence

December 11, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official response from the RCMP Special "T" Unit of Quebec City, "C" Division in the province of Quebec with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

Lawful access is an extremely important and useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorist acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorized to intercept a communication or search and seize data.

We support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications technologies. We look forward to the opportunity to continue discussions on this issue as the lawful access legislative review progresses.

Sincerely,



Daniel Morin  
NCO i/c  
Special "T" Unit  
"C" Division  
Province of Québec

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry



# Truro Police Service

K.C. MacLean - Chief of Police • G. Rogers - Deputy Chief of Police

Date: December 11, 2002

Justice Canada  
Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor,  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8.

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Truro Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Truro Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief of Police  
*Truro Police Service*

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry



Royal  
Canadian  
Mounted  
Police

Gendarmerie  
royale  
du  
Canada

Security Classification / Designation  
Classification / Désignation sécuritaire

Montreal, Quebec  
December 11th, 2002

Your file      Votre référence

Our file      Notre référence

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington street  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

This letter is in reference to the Lawful Access Consultation

Please consider this an official response from the Royal Canadian Mounted Police Special "I" Unit of "C" Division in Quebec with respect to the "Lawful Access" consultation process that ends on December 16th, 2002.

Lawful access is an extremely important and useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorists acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorised to intercept a communication or search and seize data.

We support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications

Canada



technologies. We look forward to the opportunity to continue discussions on this issue as the lawfull access legislative review progresses.

Sincerely,



Jean Martin  
Unit Commander  
Royal Canadian Mounted Police  
Special I Unit  
C division  
Montreal  
Quebec

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry



**OAK BAY POLICE DEPARTMENT**  
**THE CORPORATION OF THE DISTRICT OF OAK BAY**  
1703 Monterey Avenue, Victoria, B.C. V8R 5V6 / Phone: (250) 592-2424 / Fax: (250) 592-9988

December 11, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington Street  
Ottawa, Ontario, Canada K1A 0H8

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Oak Bay Police Department with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Oak Bay Police Department agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief Constable  
Oak Bay Police Department

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry



# Abbotsford Police Department

2838 Justice Way, Abbotsford, B.C. V2T 3P5 Phone 604-859-5225 Fax 604-859-4812

Chief Constable

Deputy Chief Constable

December 11, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor - 284 Wellington Street  
Ottawa, ON K1A 0H8  
Canada

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Abbotsford Police Department with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Abbotsford Police Department agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief Constable  
Abbotsford Police Department

Cc: Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

*In partnership with the citizens of Abbotsford, we are dedicated to ensuring safety and security by enforcing the law, preventing crime and responding to community needs.*

000239

# BROCKVILLE *Police*

[redacted]  
of Police

[redacted]  
Deputy Chief of Police



*"Partners for a Safe Community"*

BUSINESS PHONE:  
OPERATIONS FAX:  
EMERGENCY:

(613) 342-0127  
(613) 342-0452  
DIAL 911

December 11, 2002

Justice Canada  
Lawful Access Consultation,  
Criminal Law Policy Section  
5<sup>th</sup> Floor, 284 Wellington St.,  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

**RE: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Brockville Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Brockville Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

[redacted signature]  
Deputy Chief of Police

CC: Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

JM/nw



Royal  
Canadian  
Mounted  
Police

Gendarmerie  
royale  
du  
Canada

Security Classification/Designation  
Classification/désignation sécuritaire

**Unclassified**

Your File    Votre référence

Our File    Notre référence

02-12-11

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official response from the RCMP Special "T" Unit of "L" Division in Prince Edward Island with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

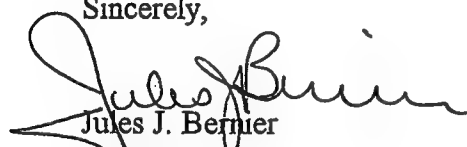
Lawful access is an extremely important and useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorist acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorized to intercept a communication or search and seize data.

We support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications technologies. We look forward to the opportunity to continue discussions on this issue as the lawful access legislative review progresses.

Sincerely,



Jules J. Bernier

Sergeant

Special "I" Unit

"L" Division

Prince Edward Island

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry



Royal  
Canadian  
Mounted  
Police

Gendarmerie  
royale  
du  
Canada

Security Classification / Designation  
Classification / Désignation sécuritaire

Montreal, Quebec  
December 11th, 2002

Your file

Votre référence

Our file

Notre référence

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington street  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

This letter is in reference to the Lawful Access Consultation

Please consider this an official response from the Royal Canadian Mounted Police Special "I" Unit of "C" Division in Quebec with respect to the "Lawful Access" consultation process that ends on December 16th, 2002.

Lawful access is an extremely important and useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorists acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorised to intercept a communication or search and seize data.

We support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications

Canada

technologies. We look forward to the opportunity to continue discussions on this issue as the lawfull  
access legislative review progresses.

Sincerely,



Jean Martin  
Unit Commander  
Royal Canadian Mounted Police  
Special I Unit  
C division  
Montreal  
Quebec

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry





# Abbotsford Police Department

2838 Justice Way, Abbotsford, B.C. V2T 3P5 Phone 604-859-5225 Fax 604-859-4812

Chief Constable

Deputy Chief Constable

December 11, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor - 284 Wellington Street  
Ottawa, ON K1A 0H8  
Canada

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Abbotsford Police Department with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Abbotsford Police Department agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief Constable  
Abbotsford Police Department

Cc: Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

*In partnership with the citizens of Abbotsford, we are dedicated to ensuring safety and security by enforcing the law, preventing crime and responding to community needs.*

000245



**RCMP**  
**Kelowna S.E. District Headquarters**

2611 Norris Road  
Kelowna, British Columbia V1X 7M1  
Telephone: (250)491-2360 FAX: (250) 491-2380

2002-12-11

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official response from the RCMP Kelowna Special "I" Unit of "E" Division in British Columbia with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

Lawful access is an extremely important and useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorist acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorized to intercept a

communication or search and seize data.

We support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications technologies. We look forward to the opportunity to continue discussions on this issue as the lawful access legislative review progresses.

Sincerely,

  
(C.W. JONES) Sgt.

N.C.O. *de*

Kelowna Special "I" Section

"E" Division

British Columbia

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Dec 12 3:00 PM  
**To:** la-al@justice.gc.ca  
**Subject:** CACP response to the Government's "Lawful Access - Consultation Document"



Lawful Access(2).doc



CACP Response.doc

Please advise receipt of this document.

Please be advised that a "hard" copy of this document will follow this date.

[REDACTED]  
CACP

Tel: 613-233-1106

Fax: 613-233-6960

**Canadian Association  
of Chiefs of Police**  
leading progressive change in policing



**Association canadier  
des Chefs de police**  
à l'avant-garde du progrès policier

December 12, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, Ontario  
K1A 0H8

Please find enclosed the Canadian Association of Chiefs of Police response to the Government of Canada's "Lawful Access - Consultation Document" dated August 25<sup>th</sup>, 2002.

Thank you for the opportunity to be involved in the consultation process.

Respectfully,

 s.19(1)



**CANADIAN ASSOCIATION OF CHIEFS OF POLICE**

**RESPONSE TO GOVERNMENT OF CANADA'S LAWFUL  
ACCESS CONSULTATION DOCUMENT**

December 16, 2002

## TABLE OF CONTENTS

FORWARD.....	1
INTRODUCTION .....	1
<b>PART I.....</b>	<b>3</b>
The Challenge .....	3
The Needs of Law Enforcement .....	4
Infrastructure Capability and Compliance .....	5
Costs Associated with Lawful Access .....	6
Regulations .....	7
Amending the Criminal Code .....	7
Data Preservation .....	8
E-Mail .....	9
<b>PART II.....</b>	<b>10</b>
<b>INFRASTRUCTURE CAPABILITY – THE REQUIREMENT TO ENSURE</b>	
<b>INTERCEPT CAPABILITY .....</b>	<b>10</b>
Capabilities Requirements .....	10
Costs.....	10
Forbearance and Compliance.....	13
Production Orders – General .....	17
Specific Production Orders .....	18
Orders to Obtain Subscriber and/or Service Provider Information .....	19
Assistance Orders.....	20
Data Preservation Orders .....	21
Virus Dissemination.....	22
Interception of E-Mail.....	23
Other Mechanisms to Provide Subscriber and Service Provider Information.....	24
<b>PART III.....</b>	<b>27</b>
<b>VIDEO INTERCEPTS .....</b>	<b>27</b>
<b>TARGET BASED COMMUNICATIONS.....</b>	<b>27</b>
Live Monitoring.....	28
Specific Issues Relating to Emerging Technologies.....	29
1. Prepaid and Pay-As-You-Go Services.....	29
2. Cross Border Interceptions .....	30
3. Telecommunication Service Providers with No Infrastructure in Canada .....	31
4. Mobile Wireless Networks and Personal Digital Assistance Services .....	31
<b>APPENDIX “A”</b>	

## FORWARD

This paper is the response of the Canadian Association of Chiefs of Police to the "Lawful Access Consultation Document" released by the Government of Canada in August of 2002. It was prepared by the Law Amendments Committee of the CACP and the Lawfully Authorized Electronic Surveillance (LAES) sub-committee. The LAES is a standing group of experts in the field of lawful access. It includes membership from federal, provincial and municipal law enforcement as well as national security agencies.

## INTRODUCTION

Police in Canada are accountable for maintaining the safety of the public through the investigation of criminal offences and the apprehension of offenders. At the core of a given police investigation is the collection and analysis of information. This information (which in some cases may be offered as evidence in a criminal trial) can take many forms. It may be in the form of witness statements, confessions, documents or electronic data. It may be collected by search and seizure. It may be gathered through interviews of witnesses or of the accused. Additionally, various legal authorities govern both how and when such information may be collected and what use may be made of it. These legal requirements are often complex and exacting in that they must respect both the privacy of Canadians as well as the complex rules of evidence in criminal proceedings. "Lawful access" is the term used to describe the conditions under which law enforcement and national security agencies can lawfully intercept private communications.

In the case of serious crime, information is sometimes collected using electronic surveillance or interception of communications. Police gather information by learning what criminals are saying to each other while they pursue their criminal enterprise. In Canada, as in other democratic countries, this aspect of police investigations occurs under a well-established and rigorous legal framework for the lawful interception of communications. This framework requires that such interception receive the prior approval of the courts and adhere to the strict procedures set out in the *Criminal Code* as well as the principles of the *Charter of Rights and Freedoms*.

However, while communications technology has continued to rapidly advance, the ability of police to retain access capabilities and gather the necessary information to detect and apprehend criminals has not. This gap in the relationship between the law and the reality of today's technology now poses a significant threat to public safety and the attenuation of police effectiveness. It is creating a safe zone where serious criminals, such as organized crime and cyber predators, can operate free from fear of detection and apprehension. It must be remembered that as law-abiding citizens make use of modern communication technology, so do serious criminals such as sexual predators, purveyors of child pornography, drug traffickers, and Internet fraud artists. High speed Internet, digital, wireless telephones and other forms of wireless communications give organized crime many of the same benefits mainstream corporations realize. While the new and emerging technologies in the modern wired world are beneficial to Canadian society, it



does not follow that the manner in which they are used will always promote the safety and well being of our communities.

Indeed, as the following points illustrate experience over recent years shows that police investigations in Canada have been seriously hampered in a number of ways: (Appendix "A" of this paper documents selected illustrative cases)

- Police have been given warrants to access the communications of suspected criminals in order to investigate murder cases, illicit trafficking and organized crime. Notwithstanding these court orders, law enforcement has not been unable to access many wireless communications because of the nature of the technological characteristics of the equipment used by some service providers, particularly wireless providers. Criminals know about these intercept limitations and exploit them.
- Toll records and subscriber information are critical to tracking criminals and have proved invaluable in many homicide investigations. However, currently there are no established standards for maintaining subscriber information and in some cases, even willing companies cannot decipher their own records.
- There are a number of examples where the safety of victims of crime has been jeopardized by the refusal of carriers to comply with existing legislation and warrants. Non-compliance and delays are serious threats to public safety.
- The internet is increasingly being used as a tool by serious criminals, including sexual predators, child pornographers, criminal organizations, perpetrators of hate crime and individuals engaged in criminal harassment, cyber-stalking and threats, in part because of the absence of effective controls and tools specifically designed to protect subscriber anonymity. Internet Service Providers have been very reluctant to provide information about registered users even when these clients are engaged in dangerous criminal behaviour. Some ISPs have also refused to cooperate with court ordered surveillance.
- Jurisdictional problems, particularly with respect to wireless transmissions across provincial and international borders, have been a significant impediment to efforts to investigate organized crime as well as cases of violent crime.
- Pay-as-you-go phones are becoming a favourite tool of criminals, as the requirements for subscriber identification are minimal. One province noted that these phones are registered to 150 "Mickey Mouses" and 30 "Donald Ducks".
- There are also many instances where emergencies have occurred, including kidnappings, suicide threats and robberies, where unreasonable delays by carriers in complying with requests for information put public safety at risk

On August 25, 2002, the Department of Justice, Industry Canada, and the Portfolio of the Minister of the Solicitor General invited interested parties to comment on the issues raised in the "Lawful Access – Consultation Document." This paper sets out the response of the Canadian Association of Chiefs of Police to those issues.

The Canadian Association of Chiefs of Police (CACP) was founded in Toronto on September 6, 1905. It was incorporated by Letters Patent under Part II of the *Canada Corporations Act* in 1968 as a non-profit organization. The Association is dedicated to the support and promotion of efficient, fair and effective law enforcement and to the protection and security of the people of Canada.

Part I of this document will outline the issues from the perspective of the Canadian law enforcement community. Part II of this document will address specific issues brought forward in the consultation paper in detail. Part III will address several ancillary issues that fall outside the consultation document but which the CACP believes ought to be included in the proposed legislation. Appendix "A" is a compendium of specific examples of the challenges faced by law enforcement and national security today.

## PART I

### The Challenge

Prior to 1974, there was no nation-wide legislation relating to the protection of private communications. At that time, various pieces of provincial legislation attempted to address lawful access in individual provinces. This patchwork of provincial laws proved to be an unsatisfactory means by which to attend to the complex, and sometimes competing, issues relating to the protection of privacy and the maintenance of public safety.

In 1974, Parliament recognized the need to protect citizens from unjustifiable intrusions into their privacy and passed the *Protection of Privacy Act*. This Act also added what is now Part VI to the *Criminal Code*. The effect of this legislation was twofold. First, it made it a criminal offence for a person to unlawfully intercept another person's private communications. Second, an exception to this prohibition was created for law enforcement agencies investigating certain offences, as long as these agencies followed the procedures set out in the legislation, which included obtaining the prior authorization of a judge. Although there have been some modifications to the legal provisions relating to lawful access since their inception in 1974, the fundamental make-up of this legislation remains essentially unchanged. Yet since that time Canadian society has seen dramatic changes in information technologies such as wireless phones, satellite phones and the Internet, which were not widely available in the 1970's.

Other significant changes have occurred since that time, which have seriously undermined the lawful access capabilities of the police. Deregulation of the telecommunications industry, global and cross border criminal activity, cyber crime and the costs associated with the software and mechanisms required to lawfully intercept

communications have significantly impaired the ability of law enforcement to use this investigative tool.

Today, Canadians live and work in a much different world than they did in 1974. The CACP therefore believes that the present laws surrounding the lawfully authorized access to communications must be updated to keep pace with advances in communications technology.

## **The Needs of Law Enforcement**

According to Statistics Canada, last year more than eight million families, or about two-thirds of the total of Canadian households, contained someone who had used the Internet at some time in their life. The use of the Internet to facilitate communications and transact day-to-day business has grown in proportions not anticipated even a short decade ago.

In 1993, there were an estimated 18 million wire-line and mobile wireless subscribers. This increased to 26.9 million by the end of 1999 and to 28.2 million by June 2000. At the same time, the share of residential wire-line access lines declined from 64% in 1993 to 46% in June 2000. The largest change relates to the number of wireless subscribers - from one million in 1990 to over 10.9 million at the end of 2001 (source: Industry Canada's telecommunications Service in Canada, An Overview: 1999-2000). We are becoming a nation of wireless communicators.

Clearly, the face of communications in Canada has undergone rapid and comprehensive change. New technologies have added much that is positive to society. Yet the rapid change and the ubiquitous nature of the new technologies present significant public safety challenges to the law enforcement community. As the average Canadian benefits from increased connectivity, so do serious criminals. As high speed Internet and the wireless world contribute to Canadian competitiveness on the global stage, so does it benefit those who seek to operate beyond the law and profit from it. Police are faced more and more with increasingly sophisticated criminals employing the latest telecommunications technologies to advance their unlawful enterprises and injurious conduct as well as frustrate police efforts to apprehend them.

This is hardly a phenomena restricted to Canada. Other democratic countries such as Australia, New Zealand, Britain and the Netherlands are ahead of our country and have adopted legislation aimed at modernizing their lawful access statutes. These countries have recognized that technology has not only provided the means by which criminals facilitate the commission of offences, it also allowed them to broaden the scope of their unlawful activities by virtually eliminating borders and geographical restrictions. Indeed, there are many examples where Canadian police strive to work collaboratively in an integrated approach within the international policing community. As far as is appropriate within the limits of the *Charter*, police powers need to be harmonized with the global context within which the law enforcement community finds itself.

There are therefore some broad principles the CACP considers very important to this discussion on modernizing and harmonizing Canada lawful access laws.

1. *The circumstances in which Canadian police may intercept private communications must continue to be the subject of prior court approval.*
2. *The technological ability to actually implement the court ordered access must always exist and never be compromised. There should be no "intercept safe havens" in Canada.*
3. *New communications technologies are not of themselves problematic. However, left unregulated and without the necessary checks and balances, they can have unintended detrimental consequences. Modern legal mechanisms are required to ensure we as a society balance the needs of global competitiveness with that of effective public safety.*
4. *Modern communication technology shrinks distances and operates free of geographical constraints. Organized criminals, Internet predators and terrorists take advantage of this fact. Legislation in Canada must reflect the increasing cross border nature of crime.*
5. *Some service providers require law enforcement agencies to pay significant fees before they will implement a court ordered interception. No persons, whether corporate or otherwise, must be permitted to erode the authority of the court by imposing fees or other financial obligations as a condition of compliance with a lawful order from the court.*

Against the backdrop of these fundamental principles arise several important challenges for law enforcement and national security agencies. The Lawful Access-Consultation Document identifies these issues and makes a number of important proposals, many of which are supported by the CACP.

### **Infrastructure Capability and Compliance**

The CACP supports a legislated requirement that all communication service providers have the technical capability to provide lawful access to the entirety of a specific communication transmitted over their facility. To be effective and meet the public interest, the requirement must apply to all communication technologies, whether wireless, Internet or wire-line.

To this end, the CACP believes that the minimum acceptable standard is for all new or significantly upgraded technologies to be intercept capable with the goal that all technologies operating in Canada, without exception, be intercept capable within a specified period of time. Additionally, while the CACP recognizes the need for forbearance of these obligations in specifically delineated circumstances, the exceptions must not be permitted to swallow the rule; such forbearance must be rare.

In order to ensure the effectiveness of the obligations imposed upon service providers, the CACP supports a compliance mechanism that is independent of government, effective, efficient, appropriately funded and resourced. In addition to compliance, this entity should be responsible for questions of forbearance while cabinet remains in an appellate position. The CACP believes it is in the interests of all Canadians that a body at arms-length make such decisions from government.

The CACP urges government to give functional effect to the legislation by putting in place effective regulations. These regulations should place specific obligations upon service providers to provide reasonable capacity for multiple simultaneous interception, as well as effective requirements for both the security of the police operations and the integrity, competence and reliability of the employees involved.

### **Costs Associated with Lawful Access**

The CACP supports the proposal that communication service providers bear the cost of creating the access capability to their new or significantly upgraded technologies. One key aspect of apportioning this cost, and to the ultimate effectiveness of the legislation, is the public policy question relating to the imposition of costs on police agencies by communication service providers. Even if the technical ability to intercept exists and the courts have authorized the intercept, many service providers have attempted to arbitrarily impose significant fees upon the police. In the past, this forced many law enforcement agencies to "negotiate" ad hoc contracts with telecommunications corporations. The legal and principled appropriateness of such agreements is highly doubtful. Furthermore, and from a purely practical perspective, the actual ability for law enforcement to pay for court ordered assistance varies greatly from jurisdiction to jurisdiction and to a large extent depends upon whether the agency in question is federal, provincial or municipal in nature.

While it is recognized that compliance with court ordered access imposes an expense upon service providers, the CACP believes that such costs relate to a "public good" and that all Canadian citizens, whether individual or corporate, have an interest in seeing orders of the court carried out. In particular, the CACP believes that assistance to law enforcement and compliance with court orders must not be viewed from a "profit" perspective, but rather from the needs of the overall public interest and public security.

Additionally, the CACP believes that it is not in the public interest that entities be permitted to circumscribe and limit the effectiveness of an order of the court by imposing an after-the-fact-fee as a precondition of compliance with that order. The CACP believes this is a challenge to the authority and effectiveness of the courts and must not, as a matter of public policy, be permitted to continue. The CACP therefore urges the government to enshrine in legislation a firm prohibition against charging fees for compliance with any court orders.

The CACP also urges the government to specifically prohibit communication service providers from directly or indirectly recovering infrastructure costs from law enforcement agencies. Other mechanisms, besides police budgets, should be considered in relation to the cost issue.

The CACP further urges the government of Canada to consider the matter of costs from a national perspective. The CACP respectfully submits that the cost of lawfully authorized access is not a solely a law enforcement issue but is akin to airport security in that it is a matter of greater importance to society at large. For this reason, any cost recovery mechanism that is established must be broadly and equitably distributed, reasonable, proportional to the actual assistance rendered, and subject to review by an independent third party. Permitting industry to arbitrarily impose costs and therefore make police operations prohibitively expensive will diminish the effect of the proposed legislation and ultimately compromise public safety.

## **Regulations**

In order for the proposed legislation to ensure an access capability, carefully drafted regulations will be required. Therefore, the CACP supports regulations, which are not only consistent with international standards, but are effective and workable in Canada. Such regulations must provide police with contemporaneous or "real time" monitoring capabilities when acting under a court authorization. This means that police need to be able to access both the content of the communication and the associated traffic data as well as the means to accurately associate the two to a standard acceptable for evidence in a criminal proceeding.

Further, in order to promote fair and successful prosecutions as well as protect the privacy rights of Canadians, the aforementioned regulations must require that service providers put in place mechanisms and procedures that allow police to focus on only those targets to whom the authorization applies. This includes obligations to ensure the privacy and security of the content of the intercepted communication, the associated data and the identities of related persons.

Finally, these highly sensitive and costly investigations must be undertaken within a tight security framework. Unauthorized or premature disclosure can jeopardize not only the investigation and subsequent prosecution, but in some cases the safety of police officers, witnesses or the targets themselves. Therefore, the regulations ought to strictly impose upon communication service providers' measures to ensure personnel and physical security of the operation.

## **Amending the *Criminal Code***

The CACP supports the proposals contained in the discussion paper concerning amending and updating the *Criminal Code*. As stated above, the CACP considers it

vitality important that the powers in the *Criminal Code* with respect to search, seizure and the interception of electronically held material be modernized.

Today, information flows quickly across boundaries, exists in simultaneous locations electronically and includes new types of information such as traffic related data. Furthermore, there are varying degrees of privacy interest that attach to these different types of information. For example, the CACP submits that there is a lower privacy interest in relation to customer name and address and the identity of a service provider clearly vis-à-vis the content of a given communication.

As for the Internet, cyber crime knows no geographical or jurisdictional boundaries. With the rising use of the Internet, especially among the young, it is imperative that police agencies be afforded the ability to trace and intercept those persons who would use the Internet to prey on children and other vulnerable members of society. The personal safety of Canadians and the vitality of our economy are at stake. At this point, the CACP desires to make it abundantly clear that we are not asking for the power to randomly and, without prior judicial authorization, monitor the Internet activities of Canadians. The ability to intercept/seize Internet based private communications and information will always be conditional upon the receipt of prior approval by the courts.

Clearly, in the face of the deregulation of the telecommunications industry and the sometimes patchwork layers of telecommunications corporations across the country, it is in the interests of public safety that the police be able to access information in a timely manner. The police require quick access in order to identify the service providers of both wire-line and wireless services for investigational purposes. Additionally, it is imperative that service providers be obligated to retain their information and populate a centralized database or establish some other mechanism that allows for timely electronic access. Not only is this important for investigational purposes within an electronic world and increasingly mobile population, it is also imperative for the purpose of emergency services and 9-1-1 tracing. Finally, the CACP considers it important that the infrastructure of the Internet be given further protection against malicious and damaging attacks through the addition of the *Criminal Code* offences of possessing, creating or selling a virus without a lawful excuse.

## **Data Preservation**

It is important to note that preservation of data is not the same as seizure of that data. Where a power is provided to temporarily order a service provider to preserve data, the ability of law enforcement to subsequently seize that data must still meet all the constitutional requirements of any other warrant. Some would say that the privacy interests attached to this data would require that any preservation order meet the test of prior judicial authorization, as with any other search warrant. However, this argument ignores the reality that such orders concern simply preserving rather than seizing data.

The CACP proposes investigating officers or certain designated officials within law enforcement agencies be authorized to issue data preservation orders on a short-term



basis. These orders would remain extant for seven business days. Before the expiry of seven business days, the police should be required to obtain judicial authorization in order to extend the preservation period. Upon such authorization being granted, the service provider would be required to preserve the data for 90 days. The CACP believes this is a balanced approach and is not unduly onerous on communication service providers. This methodology recognizes the fast and free flow of information inside and outside of Canada and the importance of having realistic tools to facilitate the gathering of information for the purposes of *bona-fide* and lawful investigations.

## **E-Mail**

With respect to search and seizure of e-mail, the CACP believes there is much uncertainty and confusion within the law. The CACP therefore welcomes the Government's proposal to clarify the existing laws as they pertain to the interception and seizure of e-mail. While the CACP believes that the content of e-mail and the seizure thereof should always be the subject of prior judicial authorization, we respectfully submit that the seizure of that material does not meet the definition and procedural requirements of an interception. Rather, e-mail is akin to a letter sent through the postal system, the seizure of which ought to be governed by the search warrant procedures of the *Criminal Code*.



## **PART II**

This part will address in detail each specific topic set out in the Consultation Document. The responses below will at times be in the form of an answer to the questions posed in the consultation document.

### **INFRASTRUCTURE CAPABILITY – THE REQUIREMENT TO ENSURE INTERCEPT CAPABILITY**

#### **Capabilities Requirements**

Regulations should set out requirements for Communication Service Providers (CSP) to provide Law Enforcement and National Security Agencies access, in real time, to the following, notwithstanding any features and/or services offered to the subscriber/customer:

1. The technical capacity to isolate the telecommunications of the subject of an interception order from any telecommunication that does not fall within the scope of that order and to provide the intercepted information only to the specified law enforcement or national security agency.
2. The technical capacity to have access to the entire telecommunications of the subject of an interception order, including content, so as to allow the authorized agency to conduct "real-time" monitoring for the full duration of the interception.
3. Access to all attempts of the subject of an interception order to establish telecommunications.
4. A means by which to accurately associate the telecommunications associated data and the call content.
5. The physical, personnel and administrative measures to ensure security in relation to interceptions.
6. CSP encryption to be delivered to the law enforcement/national security agency "en claire".
7. The transmission to law enforcement and national security agencies of the most accurate location information available to the CSP network.

#### **Costs**

The consultation document makes several references to cost issues and further uses the term "operational assistance". We must define "operational assistance". In order to do

this, we must itemize the functions required of the communication service provider by the law enforcement or national security agency when a court order is in play.

1. On page 7 of the consultation document, the issue of infrastructure capability is addressed. It infers that the proposed legislation will compel the service provider to ensure intercept capability when deploying new or upgraded communications technologies. We assume that the costs associated to this provision will be borne entirely by the service provider. Given that assumption, the regulations ought to stipulate that those infrastructure costs cannot be recovered from the law enforcement and national security agencies through any cost recovery scheme (such as buried in operational or "hook-up" costs), as has been the case.
2. Pages 9 and 10 of the consultation document address issues concerning existing systems or networks. Currently, some communication service providers charge costs to law enforcement and national security agencies for rendering the assistance ordered by a court in relation to a lawful interception. These "charges" include cost recovery for development, deployment and use of the intercept solution and use of the network. The CACP proposes that the regulations specifically prohibit this practice. A police agency operating pursuant to a specific court order is in no position to "bargain" for the development of an intercept solution or the use of a given communications network. As stated above, the CACP respectfully submits that permitting businesses to charge police agencies for court ordered assistance would set a troubling and dangerous precedent for our justice system.
3. Pages 12 and 17 refer to access to subscriber information (or Customer Name and Address (CNA), and Local Service Provider Identification (LSPID)). Currently, some communication service providers charge law enforcement and national security agencies a fee for every "look-up" even, if they are compelled to provide it pursuant to a court order.

Even if the view that police agencies are in no position to truly bargain for court ordered services is discounted along with the contention that paying for court ordered services is legally untenable and brings the administration of justice into disrepute, another important factor in this discussion should be considered. In this regard, the CRTC has recently authorized the creation of a new LSPID database on the Web, accessible by anyone without charge. It is submitted that there little if any justification for companies to charge police and national security agencies for LSPID information if an LSPID database can be provided to the public without charge. The only difference between the LSPID information that is obtained by law enforcement and the information contained in the aforementioned public database is that the former is presumably the most accurate and current data that can be obtained.

4. On occasion, court orders (search warrants or general warrants) must be obtained to acquire specific information from a service provider, which would not

ordinarily be acquired by virtue of a Dialed Number Recorder warrant or Authorization to Intercept Private Communications order. In these cases, once again there is great disparity between service providers as to what is charged back to the law enforcement and national security agencies. In some cases, the execution of the court order is achieved without the provider seeking compensation. In other cases, an hourly rate is charged. Because the information is acquired by virtue of an order from the court, it is submitted that no fee should be charged directly to the law enforcement or national security agency in question.

5. "Haulback" lines for intercepted product from the telecommunication service provider to the requesting law enforcement or national security agency are presently regulated by the CRTC, and tariffed at the same rate as business entities. As technology evolves, so do the intercept solutions requiring more bandwidth at a corresponding increase in costs. We propose that the costs associated to hauling back the information to the agency must be calculated outside any tariffed rate. The rationale for this assertion is based on the fact that the tariffed rate has a profit component built into it. Section 27 of the *Telecommunications Act* provides for carriers to reduce tariffed rates under certain circumstances. It is the CACP's position that law enforcement and national security agencies should be granted an exempt status pursuant to this provision.
6. The process of giving effect to the court order by establishing the connectivity between the target and the law enforcement or national security agency is often referred to as the "hookup". Most communication service providers charge or attempt to charge fees for "hookups". Again, because this process relates to court ordered assistance, the CACP submits that fees ought not to be charge to police or national security agencies.

On the issue of costs, three fundamental issues must be resolved:

1. Should communication service providers be paid for providing court ordered assistance?
2. If so, who should pay?
3. What factors ought to be considered when determining the appropriate fees to be paid?

As for paying communication service providers for court ordered assistance, the CACP endorses in principle the notion of cost recovery for these businesses. However, we strongly oppose the notion that individual police agencies should pay for court ordered assistance. These costs are prohibitive for most police agencies (especially municipal and provincial agencies) and would result in the compromise of public safety in many jurisdictions.

If government decides that compensation is required in relation to court ordered assistance, we recommend that payment for the costs in question be distributed as broadly

as possible. One possible option would be to attach a small security fee to the accounts of the clients of all communication service providers. The existing "911" fee serves as a model upon which this proposal could be based.

If the Government of Canada determines that it is appropriate from a public policy perspective that fees for court ordered assistance be permitted, then it must be determined which factors ought to be considered to establish appropriate costs. The CACP believes that the first and governing principle ought to be that a consistent and standard practice be applied across Canada. At the present time, the costs that the various communication service providers desire to charge law enforcement/national security agencies appears arbitrary and inconsistent.

The CACP also recommend that, if compensation is considered appropriate, it should be based on the availability of appropriately trained and security cleared personnel that are used perform the tasks associated with the court orders. Additionally, any schedule of fees that might be considered should take into account that technologies have advanced to the point where most of the tasks in question (eg., "hook-ups") can be carried out logically (in the computer circuit sense). This process is neither onerous nor time-consuming in most cases (especially given that those systems that require more work are being phased out and more streamlined mechanisms are being employed).

In conclusion, the CACP contends that police agencies should not be charged fees in relation to assistance ordered by the courts. This would not only set a troubling precedent for all kinds of warrants, most agencies simply cannot afford to pay these costs without seriously compromising their ability to investigate serious crime. If the government does believe that fees are appropriate, we respectfully submit that they ought to be distributed over a broad base (such as the aforementioned security fee) and charged on a cost recovery basis only.

## **Forbearance and Compliance**

The CACP recommends that concerns respecting compliance and forbearance must be addressed by a board or tribunal that functions at arms length from government. In this regard, the CACP has studied the compliance bodies, which have been established in the following countries:

### *United Kingdom:*

The ultimate authority to dispense rulings in the United Kingdom is the Secretary of State. In order to be fully briefed on the issues involved, the Secretary consults with a number of specific groups. One of these groups is the Technical Advisory Board. This Board obtains its mandate, direction and authority from the *Investigatory Powers Act, 2000*. The Board is designed as "an advisory, non-departmental body". It functions as a review body should a communication service provider believe that it is being asked to make unreasonable efforts to maintain an interception capability.

The Board consists of thirteen people. With the exception of the Chair, membership on the Board is evenly split between those who represent the interests of the industry and those representing the interests of the intercepting agencies. The Chair is neutral and is appointed by the House of Commons. The powers and mandate of the Board are set out in the applicable statute.

*Australia:*

The Australian government has established the Australian Communications Authority, which is principally responsible for regulating telecommunications and radio communications. The mandate of the Authority includes promoting industry self-regulation, managing the radio frequency spectrum, and overseeing consumer protection issues. The ACA was established under the *Australian Communications Authority Act, 1997* and exercises powers under the *Telecommunications Act 1997*, the *Radiocommunications Act 1992*, and other related legislation.

The ACA is governed by a group of 11 appointees and includes a total of ten different teams and groups. Any number of these teams could be called upon to assist in the resolution of a dispute with respect to the interpretation of a policy or a prior ACA decision. All in all, the ACA employs in excess of 430 individuals. Although a large organization, the ACA's responsibilities are significant and diverse.

*United States:*

The United States system allows for compliance and forbearance issues to be adjudicated by the Federal Communications Commission (FCC). The FCC relies heavily on the *Communications Assistance to Law Enforcement Act (CALEA)* Implementation Section (CIS) of the FBI.

The FCC is an independent United States government agency directly responsible to Congress. The FCC was established by the *Communications Act* of 1934 and is charged with regulating interstate and international communications that are made over radio, television, wire, satellite and cable. The FCC's jurisdiction covers the 50 states, the District of Columbia, and all U.S. possessions.

Five Commissioners appointed by the President and confirmed by the Senate for five-year terms direct the FCC. The President also appoints a Chair. As the chief executive officer of the Commission, the Chair delegates management and administrative responsibilities to the Managing Director. The Commissioners supervise all FCC activities, delegating responsibilities to staff units and bureaux. The FCC is a large bureaucracy that has numerous responsibilities over and above those outlined herein.

When reviewing these examples from other countries in light of the CACP's recommendations (described, *infra*), it is apparent that even the smallest of the aforementioned bodies (the UK's Technical Advisory Board) is larger than that which is proposed by the CACP.

The CACP is recommending adoption of one of the two following options for dealing with the issues of compliance and forbearance:

1. The Solicitor General and the Minister of Industry would have joint responsibility through an arms length body to issue a forbearance order and resolve disputes between communication service providers and law enforcement/national security agencies.
2. A Board consisting of three members appointed by Cabinet would have the authority to issue a forbearance order. The Board would consist of representatives from the Federal Solicitor General's office, Industry Canada, and the Lawfully Authorized Electronic Surveillance (LAES) sub-committee of the CACP Law Amendments Committee. A person appointed by the Solicitor General would be appointed as the Chair of the Board.

The Board would be responsible for mediating and arbitrating disputes between service providers and law enforcement or federal security agencies as they relate to the compliance and forbearance provisions of the proposed legislation. The Board could avail itself of whatever experts it may require in order to come to a resolution of the dispute or forbearance request that may arise.

In either of the above-described models, the Cabinet would have the ultimate authority to forbear. In this regard, the Cabinet would serve as an appellate body in relation to initial decisions made concerning forbearance applications (for the finite time that the forbearance process remained extant in the proposed legislation).

As public safety is the guiding principle behind this proposed legislation, the CACP proposes the inclusion of a "sunset clause" regarding any forbearance issues. It is proposed that a five-year term is reasonable. That is to say, five years after the proposed legislation receives Royal Assent, the forbearance sections will cease to operate and no further applications for forbearance will be accepted.

Whichever of the above two recommended options was chosen, important procedural issues relating to forbearance decisions would have to be included in the proposed legislation:

- a) Decisions relative to forbearance would be dealt with in a timely fashion (routinely within 90 days of receipt of the application).
- b) During the period that the forbearance application was under consideration, the petitioning service provider would not be subject to any

of the financial penalties that would be set out in the Act. In considering an application for forbearance from conditions, the following matters would have to be considered;

- i) Forbearance could not be granted with respect to any of the capabilities or portions thereof, outlined in the Infrastructure Capabilities Requirements items number 1, 2, 3, 4, and 6 (see page 9, *supra*).
- ii) Forbearance from any capability could not negatively impact public safety and could not allow for the possibility of an "Intercept Safe Haven". For the purpose of this document, "Intercept Safe Haven" is defined as:

Any technology, application or device that when used as a means of communication, by its design or through its use in conjunction with other technologies, applications, or devices, either intentionally or unintentionally, impedes, hampers or otherwise does not allow for the identification of and or the interception of the communication.

- iii) Forbearance from capabilities other than those mentioned in paragraphs (i) and (ii) could be granted in the appropriate circumstances.
- iv) On application for forbearance, the petitioning service provider would be required to submit an implementation plan outlining in detail the steps to be taken in order to meet the requirements in full. The communications service provider would have to submit progress reports on a quarterly basis.
- v) The period for forbearance could not exceed 12 months from the date of granting.
- vi) Upon the expiration of the 12-month period of forbearance, the petitioning service provider would have to either comply with the capability requirements or make application for an additional 12 months extension. Any petitions for continued forbearance would be dealt with as "new" and would be governed by all the conditions as outlined above.
- vii) Significant fines would have to be levied for non-compliance with the mandatory capability requirements. In Australia, the fines range from up to \$50,000 (in the case of a person other than a corporation), and up to \$10 million (for corporations) in the case of serious and blatant breaches of the capability standards.

In any other instance involving a corporate body, the pecuniary penalty of up to \$250,000 for each contravention would be appropriate. The United States model provides for a fine of \$10,000 per day after being served with a compliance order. The British model provides for fines and/or imprisonment for up to two years.

The CACP believes that enforcement action would be the exception rather than the rule. With law enforcement and service providers working together in a cooperative partnership, the vast majority of difficulties will be worked out. Only the most severe and blatant contraventions of the capability standards set out in the proposed legislation would result in enforcement action. It should be noted that neither the United States nor the United Kingdom have yet to impose sanctions under their respective laws.

## Production Orders – General

1. Should the *Criminal Code* be amended to allow law enforcement officials to obtain production orders in specific cases?

**Response** – We are in agreement with the rationale stated in the consultation document with respect to the need for production orders. Production orders of the nature described make practical sense in modern society. Third party custodians of information can invariably locate and produce the information sought far more efficiently and with the least amount of disruption to their operations. Additionally, documents in the control of, but not in actual possession of third parties, could be obtained through a production order even if the information in question was stored outside of Canada.

2. Should the *Criminal Code* allow for anticipatory orders (e.g. permit law enforcement agencies to monitor transactions for a specified period of time)?

**Response** – Time and again, criminal cases necessitate the use of anticipatory investigative techniques to facilitate a successful resolution. Canadian law already provides for the issuance of an anticipatory warrant by the judiciary (reference S. 487.01 and S. 529(1) *Criminal Code* and *R v. Noseworthy* (1997) 33 O.R. (3d) 641 (Ont. C.A.)).

Establishing a mechanism, such as a production order, that would empower a judge or justice to authorize the monitoring of transactions for a specific time period is both a logical and common sense proposal that is consistent with the current law. For example, in a proceeds of crime investigation the investigators may require ongoing transactional information, which is in the hands of an innocent third party (e.g. a bank). Even if the search warrant process is not triggered because the information in



question possesses only a nominal degree of confidentiality, nothing compels the third party to provide it to the authorities. In such cases, a production order is a reasonable compromise between the obligation to obtain a search warrant as opposed to free access to information that does not require any form of judicial authorization.

3. What kind of procedural safeguards should be included?

**Response** – Procedural safeguards are required in order to ensure that production orders are appropriately employed. Such orders ought to be issued by either a judge or justice who is satisfied by information on oath or solemn affirmation that the officer applying for the order is engaged in the *bonafide* execution of a lawful duty and that the order is reasonable required in order for this duty to be carried out.

Search warrants should only be required in relation to information that tends to reveal intimate details of the lifestyle and personal choices of any individual affected by the order (see *R. v. Plant* [1993] 3 S.C.R. 281).

## Specific Production Orders

Issues to be considered:

1. Should there be a specific power, parallel to that provided for in the *Criminal Code* concerning dial number recorders, to allow law enforcement and national security agencies to obtain traffic data?

**Response** – There are presently no *Criminal Code* provisions specifically relating to the collection of traffic data. The procedure that can be relied upon to facilitate the collection of information in the vein of traffic data (S. 487 *Criminal Code*) does not reflect the state of Canadian law concerning such particulars. In this regard, the privacy interests that arise respecting traffic data are relatively low in comparison to those things that require a search warrant to seize. Traffic data can be likened to DNR information with respect to the level of confidentiality that it attracts. Therefore, a specific production order for the acquisition of traffic data ought to be established which is equivalent to the process used for obtaining DNR information.

2. How should "traffic data" be defined? Should the definition of traffic data be combined with telephone-related information and addressed in the same *Criminal Code* provision?

**Response** – The CACP concurs with the definition of traffic data as set out in the consultation document referred to therein as "Telecommunications Associated Data".

In this regard, cyber crime knows no territorial boundaries. Laws on cyber crime, which closely reflect those in other nations, enhances our ability to work effectively with our international partners.

It should be noted that traffic data does not include the actual communication itself; rather, it can be likened to DNR information. Given the similarity of traffic data to DNR information, it follows that it could be included in section 492.2 of the *Criminal Code*. Additionally, we propose that section 492.2 of the *Criminal Code* be expanded to permit the acquisition of DNR and traffic data where it is reasonably suspected that the information may enable the authorities to prevent the imminent bodily harm or death of any person, even in cases which do not involve an investigation into a possible criminal offence.

3. Should other specific production orders be created under a lower standard?

**Response** – See the response to the question concerning CNA and LSPID information, *infra*.

4. What kind of procedural safeguards should be included?

**Response** – As indicated in the answer to question 1, *supra*, the same procedural safeguards that apply to the acquisition to DNR information ought to apply to the acquisition of traffic data.

## **Orders to Obtain Subscriber and/or Service Provider Information**

Issues to be considered:

1. Should there be a specific production order in relation to customer name and address, and service provider information?

**Response** – It is our position that CNA and LSPID information is not personal information that requires a judicial authorization to obtain (reference *R. v. Plant*, *supra*, and *R. v. Hutchings* [1996] 111 C.C.C. (3d) 215 (BCCA), leave to appeal to the Supreme Court of Canada dismissed [1997] S.C.C.A. No. 21, the *Personal Information Protection and Electronic Documents Act*). Nevertheless, communication service providers (CSPs, which includes both telecommunication service providers and Internet service providers) are not compelled to produce this information on request. Therefore, it is proposed that a statutory provision be created that would require CSPs to provide law enforcement agencies and national security agencies with CNA and LSPID information.

In the alternative, a production order based upon a nominal procedural threshold could be given due consideration as a possible option. In this regard, although CNA and LSPID can be lawfully produced to law enforcement agencies without the need for a court order pursuant to Section 7(3) of the *Personal Information Protection and Electronic Documents Act*, nothing compels a third party in possession of such information to disclose it to the authorities. A production order of the nature

described above could attend to the compulsion issue as well as any privacy concerns that might arise with respect the information in question.

2. Under what conditions should such information be made available and to whom?
3. What is the standard that should be required?

**Response** – The response to issues #2 and #3 is limited to the perspective of police agencies. As stated above, the acquisition of CNA and LSPID information does not require a judicial authorization. However, if a low threshold production order were established, it ought to be available to police officers under the following conditions:

Such orders ought to be issued by either a judge or justice who is satisfied by information on oath or solemn affirmation that the officer applying for the order is engaged in the *bonafide* execution of a lawful duty and that the order is reasonable required in order for this duty to be carried out.

4. Should this obligation be imposed even if the service provider is not currently collecting this information for its own purposes?

**Response** – CNA and LSPID information is critically important in order for law enforcement agencies to meet both their international obligations with respect to mutual assistance as well as their responsibilities concerning community safety. Requiring service providers to maintain CNA and LSPID records is not an unreasonable stipulation and should be made a prerequisite to conducting business operations in Canada. In this regard, corporations are not islands unto themselves. The fact that they operate in a competitive environment and are principally responsible to their shareholders ought not to relieve them from fundamental responsibilities of Canadian corporate citizenship.

## Assistance Orders

Issues to be considered:

1. Should legislation that already allows for the issuance of search warrants or the granting of interception authorizations be amended to include the possibility for a judge or justice to issue an assistance order to give effect to the warrant or authorization?

**Response** – The fact that assistance is often required by law enforcement agencies in order to facilitate the execution of a court order has previously been acknowledged by Parliament. For example, section 487.02 empowers a court to issue an assistance order. However, this section ought to be expanded to include reference to production orders as well.

2. Should assistance orders more clearly spell out the scope and limits of what a person may be required to do to give effect to the warrant or authorization?

**Response** – It is submitted that the present rendering of S. 487.02 sufficiently attends to the issue of assistance in the execution of a court order. If specific assistance is required, then it can be requested by an investigator and considered by the judge or justice in question.

## **Data Preservation Orders**

The CACP supports including a provision in the *Criminal Code* that would permit law enforcement personnel to compel the preservation of data in anticipation of obtaining a preservation order. Oftentimes exigent circumstances arise that require immediate action by the authorities that do not have the luxury of time to obtain a judge's order. There is already clear statutory precedent for such an emergency procedure (e.g. see Sections 487.11 and 529.3(1) *Criminal Code*).

Issues to be considered:

1. Should a data-preservation order apply only to stored computer data or should it also apply to paper records?

**Response** – The CACP believes that preservation orders ought to apply to both stored computer data as well as paper records. The retention periods for computer records are often different than for paper records. It is, therefore, likely that records being sought may have been disposed of in one form, but not the other by the time a law enforcement agency serves the company in question with a preservation order. There should be sufficient flexibility built into the proposed procedures that will give the authorities the capability of obtaining a retention order with respect to either form of records.

2. Under what legal standard should a data-preservation order be granted?

**Response** - Given that a preservation order simply directs the custodian of the information in question to retain it for a certain period (as opposed to disclosing it to the authorities), a high legal standard is not required. The standard ought to simply require that such orders be issued by either a judge or justice who is satisfied by information, on oath or solemn affirmation, that the officer applying for the order is engaged in the *bonafide* execution of a lawful duty and that the order is reasonable required in order for this duty to be carried out.

3. Should standards vary depending on the nature of the data?

**Response** – No. Preservation orders only require data to be conserved and protected for a specific time period. There is a fundamental difference in preventing the loss or destruction of information and the actual seizure thereof by the authorities. The

nature of the data should not determine the procedural safeguards that should apply with respect to obtaining preservation orders. The nature of the data should only be considered in relation to its acquisition rather than its preservation. In this regard, a higher standard ought to be required in relation to the acquisition of data, which tends to reveal intimate details of the lifestyle and personal choices of any individual affected by the order.

4. Who should be authorized to issue a preservation order?

**Response** – Such orders should be issued by either a Judge or Justice.

5. What is a reasonable period for a custodian of data to be compelled to preserve data: 90, 120, 180 days?

**Response** – In order to be consistent with the Council of Europe Convention on cyber crime, it is submitted that the time period for the preservation of data ought to be a maximum of 90 days, subject to subsequent extensions being granted for just cause as determined by the courts.

6. Should there be a specific penalty for non-compliance with a preservation order, or is contempt of court sufficient?

**Response** – The Criminal Code offences of “Obstruction of Justice” (S. 139(2)) and “Disobeying Order of Court” (S. 127), as well as the common law offence of contempt of court, are sufficient to attend to those circumstances where an individual or corporation deliberately breaches a preservation order.

7. For how long should a law enforcement official be able to impose a preservation order on service providers in exigent circumstances?

**Response** – A preservation order issued without judicial authorization should remain effective for at least seven business days. This would be sufficient time to prepare an application to obtain a court ordered preservation order, keeping in mind the fact that such orders will invariably be required during periods when the courts are closed (e.g. long weekends, etc.).

## **Virus Dissemination**

With society's increasing reliance on computer systems, the dissemination of computer viruses poses a grave threat to our economy, national security and to public safety.

Uncompromising legislation designed to deter this criminal activity is required. Such legislation is also required to bring Canada into line with comparable legislation in other western democracies (e.g., Council of Europe Convention on cyber crime).

## Interception of E-Mail

### Issues to be considered:

1. Should there be a specific provision in the Criminal Code in relation to how an e-mail should be acquired?

**Response** – The CACP supports the creation of a specific Criminal Code provision concerning the court-ordered acquisition of e-mail. E-mail is not only a wire-line service provided by ISPs or web-based sites, it also includes wireless devices such as digital pagers and options such as “short messaging services”. As has been identified in the consultation document, the procedure by which law enforcement officers obtain court authorizations to obtain e-mail data is presently the subject of significant uncertainty. On some occasions Part VI of the Criminal Code has been used to collect e-mail information, while in other cases a standard search warrant has been used for this purpose. A procedure dedicated to the judicially authorized acquisition of e-mails would clarify the present uncertainty and confusion in the law.

2. If such a provision should be included, what kind of procedural safeguards should be imposed?

**Response** – The procedural safeguards that ought to apply to the court-ordered acquisition of e-mail data are the same that presently apply to S. 487 search warrants.

3. Should the type of order to be obtained in order to acquire an e-mail vary depending on the stage of the communication or delivery process?

**Response** – It is submitted that the stage of transmission of an e-mail is an irrelevant consideration in determining the nature of the order that is obtained to acquire it. The ultimate issue under consideration with respect to this question is whether the real time acquisition of an e-mail should be treated the same as the electronic interception of voice communications. It is further submitted that the higher procedural safeguards that apply to the acquisition of voice communications are not required in relation to the acquisition of e-mail data. It is not whether the communication in question is processed in real time that determines its measure of confidentiality. Rather, it is the transitory nature of the communication itself that determines the degree of privacy that should reasonably be expected by the parties involved.

People participating in a conversation over a telephone/wireless phone can reasonably conclude that there will not be any copy of that conversation. This cannot be said of those communicating over the Internet. By its nature, an e-mail message is reduced to writing. An e-mail message can and often does go through several third party computer systems before it ever reaches its intended recipient. A copy of the e-mail is made at each computer that it passes through from the start to the end of the communication process. Thus, it would be erroneous to conclude that the extent of privacy that could reasonably be expected in relation to e-mails should equate to

verbal, transitory communications over wire-line/wireless telecommunication systems.

## **Other Mechanisms to Provide Subscriber and Service Provider Information**

Issues to be considered:

1. What type of mechanism, if any, should be put in place to provide law enforcement and national security agencies with up-to-date and accurate CNA and LSPID information while respecting the privacy of Canadians?

**Response** – There are two basic reasons why a mechanism ought to be established in order to provide law enforcement and national security agencies with up-to-date and accurate CNA and LSPID information:

- Reliable information is critical in order for investigators to proceed with a lawful and effective investigation; dated information is often unreliable information. It goes without saying that unreliable information cannot be used to obtain search warrants or wiretap authorizations. Additionally, if the safety of a member of the public is at stake, the police ought not to be placed in a position where they are acting on information that could be unreliable.
- In order to minimize any privacy and investigational integrity concerns that may arise with respect to requests for CNA/LSPID information made by law enforcement agencies, a distinct mechanism should be established that takes this matter into account. In this regard, if an investigator requests CNA/LSPID information from a CSP, employees of that company are alerted to the fact that the authorities are "interested" in a particular individual. An appropriately constructed mechanism could minimize, if not eliminate, this privacy concern.

It is the position of the CACP that one of two mechanisms should be established in order to provide law enforcement and national security agencies with reliable CNA and LSPID information from CSPs, while taking into account the aforementioned privacy and investigational integrity issues:

- Mandate a national database system for CNA and LSPID that would be populated by CSPs and accessible by law enforcement and national security agencies. This database could be created and maintained by a private corporation after being selected through a competitive bidding process as is currently the case in Australia.

- A distributed data system whereby requests for CNA and LSPID data made by law enforcement and national security agencies are automatically relayed to CSPs through an intermediary device and automatically replied to through this device.

Given that all law enforcement and national security agencies would benefit from either of these proposed mechanisms for obtaining CNA and LSPID, we believe the federal government should be responsible for funding, whichever system is chosen.

As for the confidentiality issue, the law provides that CNA and LSPID information is not sufficiently confidential in nature as to require law enforcement agencies to obtain a judicial authorization. However, as indicated in our response to the question concerning CNA and LSPID information, if a low threshold production order were established in relation to such information, the above noted mechanisms could be designed with security measures so as prohibit unauthorized access.

2. Should an obligation to collect such CNA information be imposed, even if the service provider does not collect this information for its own purposes? In other words, should a provider be compelled by law to collect CNA information?

**Response** – Our society has evolved such that certain technologies have become day-to-day necessities in the life of the average Canadian. For example, few would argue that motor vehicles are a basic transportation requirement for the vast majority of Canadians, including Canadian businesses. For this reason, it became necessary for the federal government and provincial governments to pass regulations with respect to the manufacture and operation of motor vehicles. It goes without saying that these regulations have resulted in the cost of motor vehicles being pushed higher than they otherwise would be in a non-regulatory environment. However, most would agree that the regulations in question are necessary to ensure the safety of the public at large.

Likewise, the use of the telephone (including wireless phones) has become a communication necessity for most Canadians. While the benefits of the telephone are immeasurable, advances in this technology have not come without some drawbacks. Criminals have learned to use modern communication technology to their advantage in facilitating their criminal activities. Just as it was necessary to regulate the motor vehicle industry in order to attend to public safety issues, so it is necessary to regulate the telecommunications industry from a public safety perspective.

In the context of the question concerning CNA information, we submit that one of the reasonable regulatory requirements that should apply to service providers is to collect CNA information.

3. Some mechanisms with respect to CNA information are already in place with respect to telephones. Should such mechanisms be created or adapted to provide similar subscriber information for Internet service providers?



**Response** – It goes without saying that, the extent the Internet is being used by criminals to victimize society has risen dramatically in recent times. It is also highly probable that this trend will continue to rise. The deleterious impact to individuals (e.g. child pornography) and to the development of our economy (e.g. Internet fraud) caused by those who engage in cyber crime cannot adequately be redressed unless effective tools are created for use by those responsible for combating these criminal activities. One of the important tools that can be provided for this purpose is to establish an obligation for ISPs to make available CNA information to law enforcement agencies.

4. Who should pay the costs of collecting, retaining and accessing this information?

**Response** – Given that this is a matter of trans-national importance it is submitted that the federal government should fund these costs or produce a mechanism to do so. Alternatively, a modest monthly security fee could be paid by subscribers in order to facilitate the process of collecting, retaining and accessing this information (akin to the 911 fee on telephone bills).

5. If a database were to be established, who should operate this database?

**Response** – As indicated above, it is submitted that a national database system for CNA information ought to be established. It is possible that such a directory could be created and maintained through a public/private partnership.

## PART III

This part addresses other concerns of the CACP with respect to lawful access issues that have not been addressed in the consultation document.

### VIDEO INTERCEPTS - Proposed Amendment to the *Criminal Code* Section 487.01(4)

Section 487.01(4) has afforded the police a valuable tool in effectively dealing with serious crime. The one negative aspect of this provision is that it limits the execution of video interceptions solely to police officers. This has placed a large strain on law enforcement resources.

In most cases, video warrants obtained under this section are part of a Part VI investigation involving audio interceptions. Trained civilian monitors are used to intercept audio communications under a Part VI authorization. Today's technology affords us the opportunity to combine both audio and video into the same collection systems. The present use of civilian monitors to intercept audio has proven to be successful in that these individuals are trained so as to be fully aware of the limitations set out in a Part VI Authorization and to properly monitor private communications. This practice has also placed fewer burdens on the investigating police officers who remain free to continue with the other aspects of their investigative plans.

In light of the foregoing, the CACP strongly recommends that section 487.01(4) be amended so as to permit video intercepts to be executed not only by a police officer, but a person acting under the direction of a police officer.

### TARGET BASED COMMUNICATIONS

When the current provisions of Part VI were passed into law, most communications that were intended to be intercepted were either wire-line telephone based or location based (such as placing a listening device in a room or vehicle). Clearly, personal communications have advanced significantly since the inception of Part VI. Criminals are now resorting to technology such as two-way pagers, wireless e-mail devices and coded numeric pagers to avoid interception by law enforcement agencies.

The present state of the law is problematic in that it lays emphasis on the location of the interception (please see sections 185(1)(e) and 186(4)(c)). Because wireless devices are obviously not limited to a geographic location (as are wire-line mechanisms such as the common telephone), location of the interception becomes immaterial. It is recommended that sections 185(1)(e) and 186(4)(c) of the *Criminal Code* be amended so as to delete any reference to the location of the interception. Instead, references in these provisions to the obligation to describe the location of interception ought to be replaced by a requirement to describe the "devices" that will be intercepted. Of course, an

interpretation of the term "device" will have to be added to Part VI. Concerns with respect to the privacy rights of innocent third parties who might also use the same devices as the subject of an authorization can be dealt with through conditions imposed by a Judge pursuant to section 186(4)(d).

Notwithstanding the aforementioned recommendation, a requirement to describe the location of an interception ought to be maintained in those cases where an entry is required to premises used by the object of an authorization in order to install a listening device. It should also be noted that the aforementioned recommendation does not preclude the operation of the procedural rules governing the interception of private communications at the office or residence of a solicitor (or any other place ordinarily used by a solicitor).

### **Live Monitoring**

Law enforcement agencies are strongly concerned with the "live monitoring" clauses that are routinely included in judicial authorizations under Part VI. The costs associated with live monitoring have become prohibitive.

The CACP questions the need for live monitoring in light of recent technological advances in interception equipment and software. Live monitoring is a judicially imposed restriction that requires an authorized person to listen in real time to an intercepted private communication, but only for as long as is reasonably necessary to determine whether the entire communication is one that may be appropriately intercepted. Live monitoring is to be contrasted with automatic monitoring where all private communications associated with a given device are automatically recorded and listened to at a later time.

It has been argued that live monitoring is less intrusive on the privacy rights of innocent third parties in that the monitor only listens to a small portion of the communication before it is "dropped". However, modern interception equipment includes the technological capacity to "block" a communication that has been automatically and completely recorded, once the person playing back the call has determined it is one that cannot be appropriately listened to in its entirety (blocking a call means to prevent the recording from being replayed past the point that it was determined it should not be listened to any further). The distinction between a call that is dropped in real time and a recorded call that is blocked is, therefore, entirely artificial in the context of privacy protection.

Some may argue that there is in fact a real difference between the "call drop" versus "call block" protocol in that the private communication in the "call block" scenario has been completely recorded whereas only the parts of a communication that have been actually heard are recorded in a "call drop" case. It should be noted, however, that the systems used in the "call block" protocol create an audit trail that records precisely how much of a given call was actually listened to. With the present technology, a court can always determine the exact point at which a given call was blocked, what part of the conversation has been heard, and how much has never been listened to.

In light of the foregoing, the CACP strongly recommends that the *Criminal Code* be amended so as to specifically dispense with the requirement of live monitoring in cases where the intercepting agency uses software and equipment that facilitates the "call block" protocol.

## Specific Issues Relating to Emerging Technologies

The telecommunications industry has advanced at a rapid rate in Canada giving Canadians unprecedented means of communicating. However, at the same time, the ability to lawfully intercept certain communications has been eroded because the applicable *Criminal Code* procedures have not kept pace with technological change.

Following are some of the challenges facing law enforcement/national security agencies today where amendments to the *Criminal Code* are necessary to alleviate safe-havens for criminal activity.

### 1. Prepaid and Pay-As-You-Go Services

One kind of telecommunications service which the CACP has identified as creating a safe haven from lawful interception falls under the category of prepaid and pay-as-you-go services. Prepaid/pay-as-you-go wireless phones, Internet access cards, Internet cafes and Internet services provided by public libraries all pose a significant obstacle to law enforcement in that the identity of the user of these services is easy to conceal from law enforcement.

For example, numerous wireless service providers offer pay-as-you-go wireless phones and top up prepaid airtime cards that can be purchased from a variety of locations, including convenience stores. Such services do not require a contract to be signed. Additionally, there are no monthly bills prepared and no credit checks undertaken with respect to the subscriber. Most importantly, this service does not require the identity of the purchaser to be verified. Accordingly, it is virtually impossible to determine whether the target of an investigation is using this particular technology. The same can be said for prepaid long-distance telephone cards (which can be used with either wire-line or wireless phones). To make matters worse, some service providers have begun to offer disposable prepaid/pay-as-you-go wireless phones for sale through gas stations and convenience stores for under \$30.00, making this type of service much less expensive and more easily accessible. For obvious reasons, cheap and easily accessible wireless phones that protect the identity of the user are very attractive to the criminal element.

Prepaid/pay-as-you-go services (along with the potential anonymity of the users thereof) are no longer limited to telephone use. Several service providers are proposing prepaid cards for Internet access. The potential wide spread use of these prepayment options and the virtual guarantee of user privacy during Internet access are alarming to law enforcement. Compounding the problems associated with such

services are the current Internet services offered by Internet cafes, public libraries and Internet kiosks? These entities permit a person to pay an up-front fee for time limited access to the Internet with no requirement, or even capability of identifying the user.

Prepaid services have attracted more than 60 % of the subscribers in most European, Latin American and South East Asian markets. North American communication providers are beginning to turn more towards prepaid services because they present themselves as a new growth opportunity. Some industry analysts believe that by 2007 prepaid users will account for more than half of the expected 1.7 billion wireless subscribers.

The problems associated with prepaid/pay-as-you-go services have already been acknowledged in Europe. Specifically, the absence of any regulations obliging the identification of the users of these services is recognized as conflicting with the need for law enforcement agencies to have lawful access to all telecommunications. The European member states are therefore seeking some regulatory requirement with respect to the identification of the users of prepaid service technology. The CACP strongly recommends that a similar regulatory obligation be established in Canada as well. In keeping with the principle that "no intercept safe havens be created" it is imperative that users of any communications technology be properly identified before the activation of any service and an accurate subscriber database be established and maintained.

## 2. Cross Border Interceptions

Telecommunications are not automatically limited to national boundaries. The following examples illustrate how this fact comprises law enforcement's ability to execute intercept authorizations:

- (a) The footprint of the GlobalStar satellite communications system overlaps the US-Canada border by a few miles. This means that, even though the object of a Canadian authorization may be physically located in Detroit, his or her wireless communication device is actually serviced by the Canadian switch in Windsor. Accordingly, the technical aspects of the intercept take place through a Canadian central office, even though the object is not physically in Canada.

Law enforcement and national security agencies require an amendment to the *Criminal Code* that would clearly allow these cross border intercepts to be legally admissible, provided that the interception in question took place by means of a telecommunication facility in Canada.

- (b) A virtually identical problem that has been described in the foregoing example exists in the wireless world. Wireless companies have switch sites near the Canada-US border that also allows for the object of an intercept to be physically in the United States, although the technical interception takes place at a central office in Canada. Therefore, the requested legislative amendment identified in the

example concerning satellite phones is required in relation to wireless devices as well.

### 3. Telecommunication Service Providers with No Infrastructure in Canada

The Canadian public can enter into service agreements with companies that, while maintaining an office in Canada, have no infrastructure present in Canada that would permit a lawful interception in this country. For example, AOL Canada is a supplier of Internet services to many Canadians. While this company has an office in Toronto, their entire infrastructure is situated in the United States. For this reason, it is not possible to execute an interception authorization in Canada.

The CACP recommends the creation of legislation that would compel all communication service providers who offer services to Canadians to have intercept capability available in Canada. Any new infrastructure costs that would arise in order to comply with this requirement should be the sole responsibility the telecommunication service provider.

### 4. Mobile Wireless Networks and Personal Digital Assistance Services

While the current licensing arrangements with Personal Communications Service (PCS) providers allows law enforcement and national security agencies to conduct lawful intercepts on their PCS mobile switches, the introduction of new wireless technologies over the past few years has presented numerous interception problems with respect to these services.

For example, the introduction of a high-speed packet data overlay network (i.e., the General Packet Radio System or 2.5 G network) into the existing PCS infrastructure has created significant hurdles with regard to interception. Simply stated, there is presently no intercept solution available for this particular technology. This problem will be exacerbated with the introduction of the very high-speed 3G mobile wireless data networks.

Similarly, the growing popularity of paging and Personal Digital Assistance (PDA) services has also created a number of issues vis-à-vis lawful interception. These products operate using proprietary algorithms, which make the lawful interception task exceedingly difficult for a service provider without the assistance of the manufacturer.

The CACP strongly recommends that communication service providers be forbidden from using any technology that precludes lawful interceptions, regardless as to whether they are the manufacturer as opposed to the purchaser of such technology.

**Appendix "A"**

**Examples of Law Enforcement Operations  
Impeded by Technological or Cost Issues**

**Table of Contents**

Introduction .....	1
Background .....	1
Inability to Intercept Wireless Technology .....	2
Subscriber Information .....	5
Non-Compliance Issue .....	6
Web-Specific Concerns .....	7
Pay-As-You-Go Phones .....	9
Time Sensitivity .....	10
Financial Constraints .....	11

## Appendix "A"

### INTRODUCTION

As indicated in the body of this report, lawful access and privacy legislation was passed into law in 1974. Lawful access, or the ability of the police to intercept private communications pursuant to a court order, is an essential tool in the prevention, investigation and prosecution of serious offences and for the investigation of security threats to Canada. However, because of rapidly changing technology and the impact of deregulation on the telecommunications industry, law enforcement has fallen dangerously behind in its ability to use lawful access as an investigative tool. This current state of affairs allows significant criminal activity to go either unnoticed or uninvestigated. Although research on the impact of new technologies and deregulation on policing is limited, the anecdotal evidence clearly demonstrates that the ability of the police to perform their duties has been significantly eroded since 1974 because use of the lawful access tool has been compromised.

### BACKGROUND

The cases set out below concern actual police investigations involving lawful access that were hindered or discontinued because of problems with technology or difficulties associated with deregulation of the telecommunications industry. Identifying details have been altered to protect the integrity of these investigations and the privacy of the persons involved.

The examples set out herein deal with nine specific areas of concern, most of which have to do with technical barriers and the inability to keep pace with the speed of evolving technologies. The other major issue that is addressed concerns the troubling issue of costs. Plainly stated, many law enforcement agencies simply cannot afford to use the lawful access technology available to them because of the escalating and unreasonable costs.



## Appendix "A"

### EXAMPLES CONCERNING THE INABILITY TO INTERCEPT WIRELESS TECHNOLOGY

Many modern-day criminals are technologically sophisticated. They know which technologies that are currently untraceable and are eager to spread the word to their associates. The inability to fully intercept this technology is having a profound impact on law enforcement's capacity to investigate serious crime.

There also continue to be difficulties with wireless interceptions across provincial and international borders. When more than one provider is involved in a lawful access authorization due to the inter-provincial or international aspect of an intercept, police often receive conflicting information as to which company is not in compliance when difficulties are experienced. These problems are even worse when dealing with international and foreign wireless operations.

#### Examples:

1. An authorization was obtained to intercept private communications during the course a drug investigation being conducted by a provincial police organization. The targets of the investigation were using certain wireless phones, which they knew could not be intercepted by law enforcement (the targets also forwarded phone calls from their "interceptable" cell phones to these phones to defeat the police). This hampered the investigation as important meetings and conversations were missed.
2. A Quebec law enforcement agency entered into an investigation of a well-organized street gang involved in trafficking weapons and drugs. The head of this group was using a wireless phone that was traceable.

This individual was arrested on a minor offence and spent several days in prison. Upon his release, he immediately obtained a different wireless phone that could not be intercepted. The agency believes other criminals this individual met while in custody instructed him that certain wireless phones could not be intercepted and that his original phone was probably being intercepted.

The fact this knowledge was shared between criminals in prison suggests the problem of intercepting these types of wireless phones will increase at a rapid pace. In this case, the investigation slowed considerably, putting the lives of innocent individuals in danger.

3. A member of an OMG (Outlaw Motorcycle Gang) used only a wireless telephone that, again, could not be intercepted (as he put it, "he could not then make a mistake"). In the result, the police were prevented from discovering who his associates were or learning about meetings and conversations dealing with drug buys and/or sales.

## Appendix "A"

4. As in the previous example, a police agency in Ontario learned that a close-knit group of drug dealers were using wireless phones that could not be intercepted. This agency met with the same result as the agency investigating the aforementioned OMG member.
5. Approximately two years ago, an agency in British Columbia requested an emergency intercept in relation to a kidnapping. All calls to the victim's family from the suspect were made using a wireless telephone, which the police were unable to intercept. For this reason, valuable evidence was lost.
6. A western Canadian police agency recently completed an extended wiretap file involving murder and organized crime. The targets of this investigation were using wireless communication devices for which there was no intercept solution available in Canada. On many occasions during the authorization, the targets were heard on wire-lines (which were being intercepted) to tell each other to use the wireless devices. This particular police agency has been involved in two other intercept files in the past two years where this and other non-interceptable wireless technology was used by the targets of the investigations.
7. In central Canada, criminals caused an explosion that demolished a business. One of the suspects was killed while another was badly injured. There was destruction in a two-block radius of the incident. Three suspects were quickly established. It took months for the investigators acquire enough evidence to obtain a Part VI authorization. When active interceptions began, the phone communications could not be intercepted because there was no intercept solution for the wireless phones they were using.

The provider did supply the DNR activity reports in relation to the phones in question. Investigators quickly identified the persons responsible for the arson. They also established a good case against one of the original suspects. All were eventually arrested and charged with conspiring to commit the offence as well as second-degree murder. DNR records demonstrated that at crucial points during this investigation, the suspects communicated among themselves with the aforementioned phones.

8. In the spring of 2002, advanced technology and security features once again prevented law enforcement from intercepting a primary target in a major crimes investigation in western Canada.
9. In the spring of 2001, a double homicide was committed in central Canada. The Regional Police force responsible for the investigation identified a number of suspects. It was soon determined that the suspects knew which phones were safe to talk on and which phones were not. The investigators would listen to the targets, and when the conversation got sensitive, the targets would instruct the caller to contact him on his "good" phone (the one that could not be intercepted). To make matters worse, it was determined that the suspects' phones were obtained using false names.

## Appendix "A"

10. In eastern Canada, a local drug dealer had a "storefront" immediately beside a mobile phone store. The salesperson at this phone store was one of the drug dealer's couriers. Every morning the phone salesperson would give the dealer a brand new wireless phone for the day. The police could not keep up with the suspect's actions in constantly changing phones and, therefore, could not undertake an interception.
11. A homicide investigation determined that the targets of lawful access authorization were using wireless phones as communication devices. They lived in a somewhat remote location in central Canada. The wireless company in this area was using an outdated switch manufactured in England that did not have any capacity to intercept calls. The wireless company's technician was more than willing to work with the police, but the technology he was working with did not allow him to do so.

An expensive "make shift" work-around was designed to deal with this issue at the time. However, this solution would not be an acceptable format for future interceptions in this location. Since there is no legislation or regulations in place that would ensure that all technology that is utilized in Canada must be intercept capable, the problem continues to exist in this location.
12. In June 2001, police in Western Canada were attempting to intercept a target on a certain wireless phone. They were unable to do so because of the recent acquisition of the company by another communication service provider. The target's telephone was routed to the switch of the second company instead of the original switcher. Technicians from both companies were unable to facilitate the intercept.
13. In February of 2002, a major police service had put a DNR on the telephone of a man who was a suspect in the shooting of a police officer. They attempted to utilize the Data Port to assist in ascertaining his location. Surveillance and intelligence placed the suspect in one city, but the Data Port incorrectly placed the usage of the telephone in yet another city in another province. This was critical information that significantly hampered the investigation.
14. In the fall of 2001, an agency in eastern Canada had several lines up in relation to a homicide file. Lines were active with two different telephone companies, although no data was delivered from either. The monitoring officers had to identify parties by voice recognition only and when the data did arrive by fax, it was not in any type of usable format. In some cases the data received by the police did not relate to the investigation in question.
15. A police agency in western Canada had an American citizen as a criminal target. The wireless phone he was using was registered in the United States and operated in 'roam' mode while in Canada. The police could not (and cannot) intercept these roaming calls.

## Appendix "A"

### EXAMPLES CONCERNING PROBLEMS WITH SUBSCRIBER INFORMATION

At the present time, Canadian telephone companies are not obliged to validate the accuracy of the subscriber information they obtain. Accordingly, obtaining such information as well as associated toll records becomes a time-consuming process at best and is often impossible.

#### Examples:

1. Subscriber records associated to organized crime targets are often falsified or non-existent. For example, large service providers will sell a block of numbers to a smaller service provider, which may be affiliated with an organized crime group. The larger provider does not have access to the subscriber information in the possession of the smaller provider. Given that there are no legal requirements for anyone who wishes to subscribe to phone service to provide a true name or identification, false names are often used.
2. In Quebec, DNRs (Dial Number Registry) relating to certain providers' customers cannot be provided beyond a six-month period due to technical limitations.
3. During the course of an authorization, an agency in western Canada required some CNA information from a service provider based in eastern Canada. Numerous attempts to obtain the information were unsuccessful as the service provider had difficulty accepting that the request was in fact coming from a police agency. Once the agency's identity was established to the satisfaction of this provider, the police agency was faxed a credit application and a fee schedule for such requests. The provider insisted that the police agency submit an application along with a completed fee agreement before any information was released. The provider also demanded a full-unedited copy of the authorization. It took further discussions to finally resolve this matter, causing the investigation to be delayed.
4. A western Canadian city had been experiencing a significant number of residential break-ins over a short period of time. A media release was made, advising people of the crimes and requesting their assistance. A number of tips were received, including one that only identified the non-published phone number of a possible suspect. Given the circumstances, there was not enough evidence to obtain a search warrant to obtain the subscriber information for this number. Thanks to a second call, the police determined an address for the aforementioned non-published phone number. The suspects were eventually arrested and a large amount of stolen property was recovered.
5. One major western Canadian city reports a certain telephone company's toll records are so unintelligible that even their technician is unable to decipher them.
6. An investigator with a western Canadian law enforcement agency served a provider with a warrant compelling it to provide historical toll records on a homicide file (the

## Appendix "A"

spring of 2001). It was imperative that the investigating officer be able to understand the toll records, as the usage of the telephone was critically important in determining the suspect's location in relation to the homicide. When the investigator approached the company to decipher the records, they were unable help him. Only after four months of sifting through the toll records, did the investigator come up with several key evidentiary points placing the homicide suspect one block from the homicide at the time in question.

### NON-COMPLIANCE ISSUE

In some cases, telephone companies are flatly refusing to comply with existing legislation and warrants. Decisions to provide information are being left to executives or managers at the telephone company, causing extraordinary difficulties between law enforcement and these businesses.

#### Examples:

1. By condition of license, an Ontario company is compelled to provide an intercept capability on their wireless network pursuant to the Solicitor General's Standards. In the region in question, the telephone company supported its network with two mobile switches. Interceptions had been provided continuously from this location since the rollout of the service approximately five years ago. Interceptions were provided to all law enforcement and the national security agency in most of Ontario from this location. Late in 2001, a third switch was added to the network. This switch became active in or about the month of November 2001.

In April 2002 both law enforcement and a national security agency became aware that there were holes in the interception coverage of this company. When confronted with this fact, the company readily admitted that there were intercept-related problems (all seemingly associated with the addition of the third switch).

A study of DNR records determined that, on some interceptions, agencies were missing 25% of the communication activity. Notwithstanding the fact that this carrier was compelled by condition of license to provide an effective interception capability, it failed to do so. It took approximately six months of meetings and the involvement of the Solicitor General's office before this problem was finally resolved.

2. A local exchange carrier in eastern Canada initially provided listed customer name and address information upon request to law enforcement without the requirement of a warrant. This is in keeping with the Terms of Service set by the CRTC for wire-line carriers. Recently, this company informed a police agency they would not provide any customer name and address information without a warrant or other court order. In this regard, it should be noted that police agencies are often not able to obtain a warrant because they are in the early stages of an investigation.

## Appendix "A"

Additionally, the very CNA information that is requested by investigators is being sought in order to develop the necessary grounds for a warrant.

3. A telecommunications service provider supplied a major Canadian police service with subscriber information up until the spring of 2000. They would not, however, provide non-published numbers. When the situation was addressed by including access to subscriber information in assistance orders, the company's response was to withdraw providing any service to the police service without a warrant endorsed in their province.
4. In December of 2001, a wireless company was served a warrant to provide toll records. To date, that information has not been produced. The company advises they are having problems with their software and are unable extract the information from their system.

### WEB-SPECIFIC CONCERNS

The advent of the Internet and web-based technology has opened new doors for the criminal element:

- In western Canada, a 13-year-old girl lured into prostitution by a 30-year-old man who lived in another city.
- In western Canada, a 14-year-old girl lured into stripping for child pornography videos over the web by an older man in a different country.
- In western Canada, 14-year-old girl who ran away from home with a 28-year-old man she had been writing love letters to on the web. The man was from the U.S. and drove to the girl's home to take her away.
- In central Canada, a man was charged with several counts of sexual assault, forcible confinement and impersonating a police officer when he lured young girls into meeting him through an Internet chat room.
- A woman living in Central Canada was the victim of hate mail on the web by a stalker. She received several e-mails from a person who had gained very private information about her and was using it to scare, harass and stalk her. This man, who was from another country, even put her photo and address on the web saying she was an available call girl.
- In eastern Canada, residents of several small towns received anti-Semitic hate mail over the local ISP. The hate literature contained racist material and blamed Jews and gays for world problems.

## Appendix "A"

### Examples:

1. A Quebec police agency reports that certain Internet providers offer to their customers' use of an "anonymizer". An anonymizer is a service that permits people to surf the web anonymously. This service prevented the police agency from executing warrants to find the targets of a child pornography investigation. The company claimed that even they could not identify the customers using this service.
2. Local providers in one eastern Canadian city refuse to provide logs, stating they are deleted after four days.
3. Some ISP providers in central Canada are very reluctant to make their network compliant to judicially authorized interception. Devices are now currently available for this purpose and some ISP providers have made their network compliant in this regard. During a large-scale drug investigation into an organized crime group, where the criminals were known to excel at avoiding electronic surveillance, police have had to disclose techniques during past prosecutions. A great deal of money had been invested into this investigation. Three months into the investigation, police identified an Internet service utilized by what appeared to be a key target of the group. Intercepting the electronic communications of this target would have been helpful.

After repeated requests, the ISP agreed to install a device on their network. In this regard, they would only "permit" installation if they were satisfied the investigation was necessary (a Vice President of their corporation made the decision). The device was installed with the assistance of a company technician (technical problems are being experienced with respect to this particular interception).

It should also be noted that some ISPs steadfastly ignore requests of police to work with them to create an effective intercept capability.

4. On March 5, 2002, the German Federal Police were able to convince a suspect to transmit images of hard-core child pornography to them while they were operating undercover on the Internet. The IP address was obtained. The IP address belonged to one of the larger Internet providers in Canada.

Through Interpol, the local police were requested to assist in the investigation. The local police requested the assistance of the ISP. The ISP informed the police that it could not search for records that were over thirty days old (fifty days had transpired since the German Police had commenced their sting operation). Because the applicable records were not retained past thirty days, the investigation collapsed.

5. Divisional investigators in a central Canadian city were called upon to investigate a company that was victimized by unlawful access to their database. The suspects, possibly ex-employees, were able to utilize a valid user identity and appropriate password to gain access to the database. The person responsible for this crime left a series of ISP addresses from another large Internet Service Provider who was

## Appendix "A"

prepared to provide the police with a substantial number of access records. However, as a condition precedent to providing this assistance, the police were told that they would have to obtain a search warrant and pay the ISP several thousand dollars. The condition of payment brought the case to a standstill.

6. In the summer of 1999 a homicide occurred in central Canada. The Regional Police soon identified a number of suspects and made an application for a Part VI authorization. Most of the suspects were residents of a university and were extremely computer literate. When the suspects had any phone conversation relating to the incident, they would tell each other to switch to e-mail. It was further learned that the suspects would also log onto the police web site to update themselves on the investigation. The police department did not have the ability to perform e-mail intercepts, nor the money required to purchase a system that could.
7. In a sexual predator case, a 33 year old male struck-up a relationship with an 11 year old female victim over the Internet using various "chat room" sessions. The accused promised the victim he would take her on a "shopping spree". The victim agreed to meet with the perpetrator at a certain place and readily entered the accused's vehicle on his request. He drove her to a hotel.

When hotel staff challenged the perpetrator as to his relationship with the victim, the accused decided not to rent a room and instead took the victim to his residence. The victim was sexually assaulted on numerous occasions. The accused eventually took the victim to a subway station and instructed her to return home. The victim had been reported missing the previous night by her worried parents. Police officers involved in searching for her located the victim when she got off a public transit bus near her home. She was immediately transported to the hospital for treatment.

In order to facilitate the investigation, the traffic data records of the accused's ISP were searched. The ISP in this case only had a thirty-day retention schedule. For this reason, there may have been evidence lost to not only support the case against the accused in this particular incident, but also to identify other possible victims and, therefore, investigations.

### PAY-AS-YOU-GO PHONES

A great deal of time and money are spent attempting to identify criminals who provide false information in obtaining pay-as-you-go phones. It would be beneficial to law enforcement to put into place a central registry where a subscriber's name is cross-referenced to the purchaser's real name.



## Appendix "A"

### Examples:

1. An agency in western Canada deals with many criminals using pay-as-you-go phones. Many of these individuals purchase these phones under fictitious names (i.e. Mickey Mouse, Donald Duck). Because of the use of fictitious names, police agencies are required to spend valuable resources trying to identify the phone numbers and electronic serial numbers for the phones in question.
2. One province has determined that there are 150 "Mickey Mouse's" and 50 "Donald Duck's" who have purchased pay-as-you-go phones.

### TIME SENSITIVITY

An ongoing problem experienced by law enforcement agencies across the country relates to the "business hours" of communication service providers. This issue, because of the time zone differences, particularly affects law enforcement agencies that have to deal with communications service providers located in the opposite ends of the country. Additionally, the disparity in business hours as between law enforcement agencies and service providers (round the clock police operations as opposed to 8:00AM - 5:00PM hours for CSPs) often result in the compromise of criminal investigations.

### Examples:

1. A police agency in eastern Canada attempted to perform an emergency authorization relating to an extortion file, where the victim was receiving demands on a personal wireless phone. The communications service provider advised the police agency it would have to purchase a landline in Montreal and then request the RCMP in Montreal to make the connections. By the time a connection could have been made, the emergency authorization expired.
2. A western Canadian police agency was contacted at about 9:30 p.m. last year regarding a suicidal person. A distraught female was threatening suicide to a friend during a call on her wireless phone. The police requested the relevant communication service provider to supply them with the wireless site information for victim's phone in an effort to locate her. After several conversations with the wireless service provider, the police were told that the information would not be released without a warrant. It should be noted that it is legally impossible for the police to obtain a warrant in relation to these circumstances (threatening suicide is not a crime). The information was finally obtained an hour later. The time delay from the last phone call to obtaining the information was 1½ hours and was not useful in determining the current location of the suicidal female.
3. An anonymous call was received where a person provided a non-published phone number regarding the current whereabouts of a robbery suspect who was actively avoiding arrest. The suspect had already committed a recent robbery where a victim was stabbed during the offence. Strong indications were the subject would

## Appendix "A"

re-offend. The caller advised the suspect would be at the location for a short period of time. The CNA information for this non-published number was, unfortunately, not obtained from the communication service provider quickly enough.

4. In the spring of 2002, a major police agency was dealing with an imminent and illegal transfer of an illicit firearm. It was outside ordinary business hours and the supplier of the gun was using a wireless phone. When the service provider's after-hours emergency number was contacted, the person who responded to the subscriber request would not provide it over the telephone. They stated the information had to be faxed to them. The information was faxed and was then returned two hours later. By that time, the police had to take action without the benefit of the intelligence they could have received from the service provider had the requested information been forthcoming in a timelier manner.

### FINANCIAL CONSTRAINTS

Many police agencies cannot afford intercept technology. Those that can must make decisions on a daily basis whether a project is "worthy" of spending funds on intercepts. These decisions can often involve potential life or death situations.

#### Example:

1. An agency in a Canadian city requested technical surveillance on a group of suspects thought responsible for a number of violent crimes. Although Part VI standards were met, the cost estimates for the intercept aspects of this investigation alone exceeded \$400,000.00. Officers were instructed to attempt to solve the case by other means. The worst-case scenario transpired. This group of suspects killed an innocent citizen during a botched robbery.

**Pierlot, Paul**

---

**From:** policeservice\_weyps  
**Sent:** 2002 Dec 12 11:17 AM  
**To:** la-al@justice.gc.ca  
**Subject:** Lawful Access Discussion Paper

Weyburn Police Service  
Box 776  
Weyburn, Saskatchewan  
S4H 2K8

December 12, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington Street  
Ottawa, Ontario, Canada  
K1A 0H8

Dear Minister Cauchon:

**RE: Lawful Access Consultation Document Response**

Please consider this an official and final response from Weyburn Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canada Association of Chiefs of Police (CACP). The Weyburn Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief of Police  
Weyburn Police Service

WSM

2002-12-18

000295

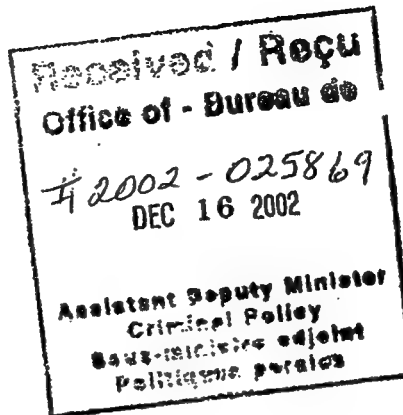


Royal Canadian Mounted Police  
Gendarmerie royale du Canada

Security Classification/Designation  
Classification/désignation sécuritaire

Unclassified

NCO i/C "J" Division Special "I"  
New Brunswick



Your File      Votre référence

Our File      Notre référence

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, Ontario

02-12-12

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official response from the RCMP Special "I" Unit of "J" Division in New Brunswick with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

Lawful access is an extremely important and useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorist acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorized to intercept a communication or search and seize data.

We support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications technologies. We look forward to the opportunity to continue discussions on this issue as the lawful access legislative review progresses.

Sincerely,

  
D.R. Domenie, Sgt  
NCO i/C "J" Division Special "I"  
New Brunswick

C.C. Honourable Wayne Easter  
Solicitor General of Canada  
Honourable Allan Rock  
Minister of Industry

Canada

# Chatham-Kent Police Service

Headquarters - Chatham

Chief of Police

Chef de Police



P.O. Box 366  
24 Third Street  
Chatham, ON N7M 5K5  
Telephone: 519-436-6600  
Admin. Fax: 519-436-6643  
General Fax: 519-352-0507

December 12, 2002

Justice Canada,  
Lawful Access Consultation,  
Criminal Law Policy Section, 5<sup>th</sup> Floor,  
284 Wellington Street,  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

**RE: LAWFUL ACCESS CONSULTATION DOCUMENT RESPONSE**

Please consider this an official and final response from the Chatham-Kent Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Chatham-Kent Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief of Police,  
Chatham-Kent Police Service.

cc: Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

# Régie intermunicipale de police Vallée-du-Richelieu

Le 12 décembre 2002

Justice Canada  
Consultation sur l'accès légal  
Section de la politique en matière de droit pénal  
284 Wellington, 5<sup>ème</sup> étage  
Ottawa (Ontario) K1A 0H8

**OBJET: RÉPONSE AU DOCUMENT DE CONSULTATION SUR L'ACCÈS LÉGAL**

Monsieur le Ministre Cauchon,

Veillez considérer cette lettre comme une réponse officielle et finale de la part de la *Régie intermunicipale de police Vallée-du-Richelieu* relativement au processus de consultation sur l'accès légal se terminant le 16 décembre 2002.

Nous avons eu l'opportunité de consulter la réponse soumise par l'Association Canadienne des Chefs de Police. La *Régie intermunicipale de police Vallée-du-Richelieu* est d'accord et supporte cette réponse au document de consultation.

Veillez agréer, monsieur le Ministre, l'expression de nos sentiments les meilleurs.

Le directeur

s.19(1)

BL/sr

C.c. ♦ Honorable Wayne Easter  
Solliciteur général du Canada

♦ Honorable Allan Rock  
Ministre de l'Industrie

Pierlot, Paul

---

From: [REDACTED]  
Sent: 2002 Dec 12 7:01 PM  
To: 'la-al@justice.gc.ca'  
Cc: Al Sauve (RCMP)

s.19(1)



Lawful Access Support  
Letter.d...

**CONFIDENTIALITY CAUTION:**

This message is intended only for the use of the individual or entity to which it has been addressed and may contain information that is privileged and confidential. If you are not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If this communication has been received in error, respond immediately via telephone or return e-mail, and delete all copies of this material.

Please accept the attached letter as my response to the Lawful Access Consultation Document.

<<Lawful Access Support Letter.doc>>

Yours truly,

[REDACTED]  
Major Crimes Division  
Edmonton Police Service

Justice Canada  
December 12  
Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor,  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8.

2002

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

I am the Superintendent in charge of the Major Crimes Division of the Edmonton Police Service. Major Crimes Division is responsible for investigating the most serious crimes against persons (homicide, child abuse, sexual assault, etc.). It has become apparent to me and my colleagues that the confluence of the following three significant factors has seriously diminished our capacity to successfully investigate these crimes: deregulation of the telecommunications industry, escalating costs of investigations utilizing lawful access techniques, and criminal procedures which have not kept up with the advances in telecommunication technologies.

I have studied both the Lawful Access Consultation document and the response to this paper that has been submitted by the Canadian Association of Chiefs of Police. In my view, the CACP's response correctly identifies the problems facing law enforcement with respect to the issue of lawful access. Additionally, I believe the CACP's response balances the need to respect the privacy of Canadians with the need for Canadians to be protected from serious criminal activities.

In light of the foregoing, I strongly urge you to give favourable consideration to the comments made by the Canadian Association of Chiefs of Police in the aforementioned response to the lawful access consultation document.

Yours truly,

s.19(1)

  
Superintendent i/c Major Crimes Division  
Edmonton Police Service



not an email from

**YAHOO!**  
**CANADA**

today is December 12, 2002  
to Criminal Law Policy Section @  
fax # (513) 941-9310

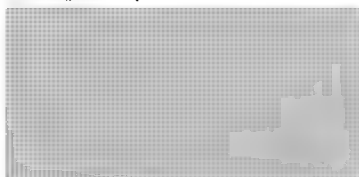
s.19(1).

from  Yahoo! Canada  
pages 1 (including this cover)  
regarding Lawful Access Consultation Document

Hello,  
Can you please advise whether Yahoo Canada can submit its comments in confidence. As we are not part of a large industry organization, we would rather not submit our comments for public view.

You can either call, email or fax with your response.

Regards,



Do You  
**YAHOO!?**

[www.yahoo.ca](http://www.yahoo.ca)

106 front street east, suite 200 • toronto, ontario M5A 1E1  
phone (416) 341-5246 • fax (416) 341-5294 • 1-800-262-3917

FOI-025649  
CLP & CJ-CLP

## CN Police

Chief

Canadian National  
935 de La Gauchetière West, 11<sup>e</sup> floor  
Montreal, Québec, Canada  
H3B 2M9  
Telephone: (514) 399-6220  
Facsimile: (514) 399-8846

## Police du CN

Chef

Canadien National  
935 de La Gauchetière O.,  
11<sup>e</sup> étage  
Montréal (Québec) Canada  
H3B 2M9  
Téléphone: (514) 399-6220  
Télécopieur: (514) 399-8846

jeudi, 12 décembre, 2002

150027

Justice Canada  
Consultation sur l'accès légal  
Section de la politique en matière de droit pénal  
284 Wellington  
5<sup>ème</sup> étage  
Ottawa, Ontario, Canada, K1A 0H8

Monsieur le ministre Cauchon :

**Re : Réponse au document de consultation sur l'accès légal**

Veillez considérer cette lettre comme une réponse officielle et finale de la part de la Police du Canadien National relativement au processus de consultation sur l'accès légal se terminant le 16 décembre 2002.

Nous avons eu l'opportunité de consulter la réponse soumise par l'Association Canadienne des Chefs de Police. La Police du Canadien National est d'accord et supporte cette réponse au document de consultation.

Veillez agréer, monsieur le Ministre, l'expression de mes salutations distinguées

s.19(1)

  
Chef  
Police du Canadian National

C.C. Honorable Wayne Easter  
Solliciteur général du Canada

Honorable Allan Rock  
Ministre de l'industrie

DEC.12.2002 11:23AM

CN POLICE CHIEF OFFICE

**CN**

**Police**

Canadian National  
935 De La Gauchetière Street West  
Montreal, Québec, Canada  
H3B 2M9

**Police**

Canadien National  
935, rue De La Gauchetière ouest  
Montréal (Québec) Canada  
H3B 2M9

s.19(1)

Date/date : 12/12/02

To: **Ministre Martin Cauchon**  
Destinataire : **Ministre Allan Rock**  
**Ministre W. Easter**

From:  
Expéditeur :

Fax No.: 613/995-0114  
Télécopieur : 613/992-0302  
613/991-4669

Fax No.:  
Télécopieur :

(514) 399-8846

Tel.:  
Téléphone :

Tel.:  
Téléphone :

(514) 399-6220

Number of pages, including this one:  
Nombre de pages, couverture comprise :

2

**CONFIDENTIAL**

*This facsimile (including all accompanying documents) may contain confidential information and may be protected by solicitor-client privilege.*

*It is intended for use by the person to whom it is addressed only. Any other use, distribution or copying is strictly prohibited.*

*If received in error, notify us immediately by telephone (collect) and return original transmission by mail without making a copy.*

**CONFIDENTIEL**

*Cet envoi par télécopie (y compris tous les documents qui l'accompagnent) peut contenir des renseignements confidentiels et peut être protégé par le secret professionnel.*

*Il est destiné uniquement à la personne à qui il est adressé. Toute autre utilisation de cette documentation ainsi que sa distribution ou reproduction est strictement prohibée.*

*Si vous l'avez reçu par erreur, veuillez nous aviser immédiatement par téléphone (à frais virés) et nous en retourner l'original par la poste sans en faire de copie.*

Tel que demandé.

MINISTER OF JUSTICE  
MINISTRE DE LA JUSTICE  
RECEIVED - REÇU

DEC 12 2002

Ministerial Correspondence Unit / Unité de la Correspondence Ministérielle  
Routing Slip / Feuille de controle

Letter/Lettre Date: 2002-12-12

s.19(1)

DEC 16 2002

Author/  
Auteur:

VIP

Document: 2002-025649

Chef  
Police du Canadian National  
935 de La Gauchetiere Ouest, 11e étage  
Montreal QC  
H3B 2M9

Doc Type/Type de Doc: F

File / Classer: 150027  
LAW - LAWFUL ACCESS

Referred To/Transmis a: CLP&CJ-CLP

Date: 2002-12-13

Due Date/Date d'échéance:

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

Additional Comments / Remarques additionelles:

*Dec 12/02*

*→ Lucie Angers*

*DL*

CC:  
CC:

CC:  
CC:

CC:  
CC:

CC:  
CC:

Closed / Fermer: 2002-12-13

File Away / Classer:

Description of type / Description des types

D: yellow docket / dossier jaune (draft response / projet de réponse)

A: further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

: follow-up at your discretion / donner suite à votre discrétion

: for your information (no action required) / à titre d'information (aucune mesure requise)

12/12/2002 15:31 506-648-3304

S.J. POLICE ADMIN.

Saint John Police Force

Chief of Police

P.O. Box 1971  
Saint John  
New Brunswick  
Canada E2L 4L1

506 648-3200  
Fax  
506 648-3304 Admin  
506 632-6158 Major Crime  
506 632-6155 District 1  
506 658-2839 Records

December 12, 2002  
SJPF File No: 160-C2-1

F02-025661  
CLP&CJ-CLP

150027



POLICE

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington Street  
Ottawa, ON  
K1A 0H8

Dear Minister Cauchon:

**Subject: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Saint John Police Force with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Saint John Police Force agrees and supports the submission in whole.

Yours truly,

s.19(1)

CHIEF OF POLICE

C: Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

12/12/2002 15:31 506-648-3304

S.J.POLICE ADMIN.

PAGE 01/02

s.19(1)

Saint John Police Force

Chief of Police

PO Box 1971  
Saint John  
New Brunswick  
Canada E2L 4L1

506-648-3200  
FAX:  
506 648-3304 Admin  
506 632-6148 Major Crime  
506 632-6155 District 1  
506 658-2839 Records



POLICE

**TELECOPIER MESSAGE TRANSMITTAL  
LEAD SHEET**

**THIS TRANSMISSION CONSISTS OF** 1 **PAGES, PLUS LEAD SHEET.**

**TO:** Justice Canada

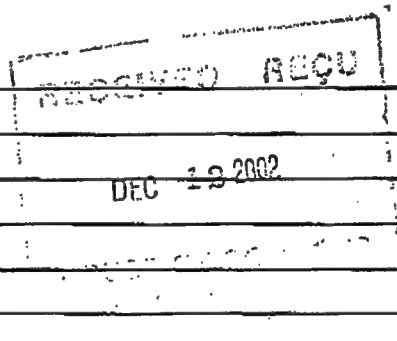
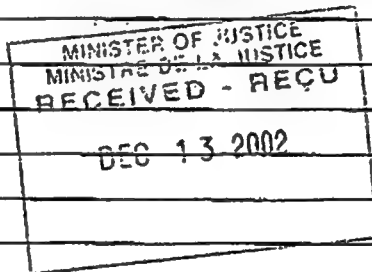
**ATTENTION:** Minister Cauchon

**FAX NO:** 1-613-995-0114

**FROM** C.E. (Butch) Cogswell, Chief of Police

**SAINT JOHN POLICE FORCE ADMINISTRATION  
FAX # (506) 648-3304**

**SUBJECT:** Lawful Access Consultation Document Response



**DATE:** December 12, 2002

**TIME:** 3:30 p.m.

**SENT BY:**

Original to follow

[ ] Yes

[ x ] No

**CONFIDENTIALITY NOTE:** THE INFORMATION CONTAINED IN THIS FACSIMILE MESSAGE IS LEGALLY PRIVILEGED AND CONFIDENTIAL INFORMATION INENDED ONLY FOR THE USE OF THE INDIVIDUAL OR ENTITY NAMED ABOVE. IF THE READER OF THIS MESSAGE IS NOT THE INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED TDHAT ANY USE, DISSEMINATION, DISTRIBUTION OR COPY OF THIS FACSIMILE IS STRICTLY PROHIBITED. IF YOU HAVE RECEIVED THIS FACSIMILE IN ERROR, PLEASE IMMEDIATELY NOTIFY US BY TELEPHONE AND RETURN THE ORIGINAL MESSAGE TO US BY MAIL AT THE ABOVE ADDRESS. THANK YOU.

Ministerial Correspondence Unit / Unité de la Correspondence Ministérielle  
Routing Slip / Feuille de controle

DEC 16 2002

Letter/Lettre Date: 2002-12-12

s.19(1)

Author/  
Auteur:

Chief of Police  
Saint John Police Force  
P.O. Box 1971  
Saint John NB  
E2L 4L1

VIP

Document: 2002-025661

Doc Type/Type de Doc: F

File / Classer: 150027  
LAW - LAWFUL ACCESS

Referred To/Transmis a: CLP&CJ-CLP

Date: 2002-12-13

Due Date/Date d'échéance:

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

Additional Comments / Remarques additionelles:

*Dec 17/02*  
*→ Lucie Angers*  
*Dr*

CC:  
CC:

CC:  
CC:

CC:  
CC:

CC:  
CC:

Closed / Fermer: 2002-12-13

File Away / Classer:

Description of type / Description des types

D: yellow docket / dossier jaune (draft response / projet de réponse)

A: further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

follow-up at your discretion / donner suite à votre discrétion

for your information (no action required) / à titre d'information (aucune mesure requise)

## Our Vision

To Be the Best Police Service,  
Providing the Highest Standard of Professionalism,  
in Partnership with Our Community



**PROFESSIONAL, FRIENDLY  
and  
HELPFUL**

Chief of Police  
Deputy Chief of Police

500 Water Street, P.O. Box 2050, Peterborough, Ontario K9J 7Y4  
(705) 876-1122 Fax Executive (705) 876-6005 Fax Operations (705) 743-1540

December 12, 2002

Faxed December 12, 2002 - 1-613-995-0114

Justice Canada  
Lawful Access Consultation  
Criminal law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, ON K1A 0H8

F02-025663  
CLP&CT-CLP

150027

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Peterborough Lakefield Community Police Service with respect to the "Lawful Access" consultation process that ends on December 31, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Peterborough Lakefield Community Police Service agrees and supports the submission in whole.

s.19(1)

Sincerely,

MINISTER OF JUSTICE  
MINISTRE DE LA JUSTICE  
RECEIVED - REÇU

DEC 13 2002

Chief of Police

cc: Honourable Wayne Easter  
Solicitor General of Canada - Fax 1-613-991-4669

Honourable Allan Rock  
Minister of Industry - Fax - 1-613-992-0302

DEC 12 2002  
HOUSE OF COMMONS  
CHAMBER OF COMMONS



Ministerial Correspondence Unit / Unité de la Correspondence Ministérielle  
Routing Slip / Feuille de controle

Letter/Lettre Date: 2002-12-12

s.19(1)

DEC 16 2002

Author/  
Auteur:

VIP

Document: 2002-025663

Chief of Police  
Peterborough Lakefield Community Police  
500 Water Street, P.O. Box 2050  
Peterborough ON  
K9J 7Y4

Doc Type/Type de Doc: F

File / Classifier: 150027  
LAW - LAWFUL ACCESS

Referred To/Transmis a: CLP&CJ-CLP

Date: 2002-12-13

Due Date/Date d'échéance:

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

Additional Comments / Remarques additionnelles:

Dec 17/02  
→ Lucie Angers

Dal

CC:  
CC:

CC:  
CC:

CC:  
CC:

CC:  
CC:

Closed / Fermer: 2002-12-13

File Away / Classer:

Description of type / Description des types

D: yellow docket / dossier jaune (draft response / projet de réponse)

A: further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

F: follow-up at your discretion / donner suite à votre discrétion

I: for your information (no action required) / à titre d'information (aucune mesure requise)

12/12/2002 15:31 506-648-3304

S. J. POLICE ADMIN.

Saint John Police Force

Chief of Police

P.O. Box 1971  
Saint John  
New Brunswick  
Canada E2L 4L1

506 648-3200  
Fax  
506 648-3304 Admin  
506 652-6158 Major Crime  
506 632-6155 District 1  
506 658-2839 Records

December 12, 2002  
SJPF File No: 160-C2-1

F02-025661  
CLP&CJ-CLP  
150027



POLICE

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington Street  
Ottawa, ON  
K1A 0H8

Dear Minister Cauchon:

**Subject: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Saint John Police Force with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Saint John Police Force agrees and supports the submission in whole.

Yours truly,

[Redacted signature block]

s.19(1)

CHIEF OF POLICE

C: Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry



EDMONTON  
POLICE  
SERVICE

F02-025659  
CUP&CT-CLP

9620 - 103A AVENUE  
EDMONTON, ALBERTA  
CANADA T5H 0H7  
PH: (780) 421-3333  
www.police.edmonton.ab.ca

150027

2002 December 12

Forwarded by Fax: (613) 995-0114

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
284 Wellington Street, 5<sup>th</sup> Floor  
Ottawa, ON K1A 0H8

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Edmonton Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Edmonton Police Service agrees and supports the submission in whole.

Yours truly,

s.19(1)

Chief of Police

cc: Honourable Wayne Easter  
Solicitor General of Canada  
fax: (613) 991-4669

Honourable Allan Rock  
Minister of Industry  
fax: (613) 992-0302



**EDMONTON POLICE SERVICE**  
**FAX COVER SHEET**9620 - 103A Avenue  
Edmonton, Alberta  
Canada T5H 0H7  
(780) 421-3333

**CONFIDENTIALITY CAUTION:** This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged and confidential. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone and return the original message to us at the below address at our cost.

Fax Number

(613) 995-0114

Destination

JUSTICE CANADA

Attention of

LAWFUL ACCESS CONSULTATION

CRIMINAL LAW POLICY SECTION

Message From

s.19(1)

CHIEF OF POLICE

Unit

Office of the Chief

Number of Pages

2

including this cover page

FAX NUMBER

(780) 421-2211

Date

2002 DEC 12

PLEASE  
CONFIRM  
RECEIPTYES ☐NO ☐

Comments

Authorized By

(780) 421-3461

COMMITTED TO COMMUNITY NEEDS

Feb. 1999

Ministerial Correspondence Unit / Unité de la Correspondence Ministérielle  
Routing Slip / Feuille de controle

Letter/Lettre Date: 2002-12-12

s.19(1)

DEC 16 2002

Author/  
Auteur:

VIP

Document: 2002-025659

Chief of Police  
Edmonton Police Service  
9620 - 103A Avenue  
Edmonton AB  
T5H 0H7

Doc Type/Type de Doc: F

File / Classer: 150027  
LAW - LAWFUL ACCESS

Referred To/Transmis a: CLP&CJ-CLP

Date: 2002-12-13

Due Date/Date d'échéance:

ACTION AT YOUR DISCRETION	<input type="checkbox"/>	DONNER SUITE À VOTRE DISCRÉTION
COMBINE WITH (SEE COMMENTS)	<input type="checkbox"/>	JOINDRE AVEC (VOIR REMARQUES)
DRAFT RESPONSE	<input type="checkbox"/>	FAIRE UN PROJET DE RÉPONSE
DIRECT REPLY WITH COPY TO MCU	<input type="checkbox"/>	POUR RÉPONSE ET COPIE À L'UCM
NOTE AND RETURN	<input type="checkbox"/>	NOTER ET RETOURNER

Additional Comments / Remarques additionnelles:

*Dec. 17/02*

*→ Lucie Anger*

*del*

CC:  
CC:

CC:  
CC:

CC:  
CC:

CC:  
CC:

Closed / Fermer: 2002-12-13

File Away / Classer:

Description of type / Description des types

D: yellow docket / dossier jaune (draft response / projet de réponse)

A: further letter to be joined with a previous document / nouvelle lettre à joindre à un document précédent

follow-up at your discretion / donner suite à votre discrétion

for your information (no action required) / à titre d'information (aucune mesure requise)

**Our Vision**

To Be the Best Police Service,  
Providing the Highest Standard of Professionalism,  
in Partnership with Our Community



**PROFESSIONAL, FRIENDLY  
and  
HELPFUL**

Chief of Police  
Deputy Chief of Police

500 Water Street, P.O. Box 2050, Peterborough, Ontario K9J 7Y4  
(705) 876-1122 Fax Executive (705) 876-6005 Fax Operations (705) 743-1540

**December 12, 2002**

**Faxed December 12, 2002 - 1-613-995-0114**

Justice Canada  
Lawful Access Consultation  
Criminal law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, ON K1A 0H8

*FOI-025663  
CLP&CT-CLP*

*150027*

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Peterborough Lakefield Community Police Service with respect to the "Lawful Access" consultation process that ends on December 31, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Peterborough Lakefield Community Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief of Police

cc: Honourable Wayne Easter  
Solicitor General of Canada - Fax 1-613-991-4669

Honourable Allan Rock  
Minister of Industry - Fax - 1-613-992-0302

MINISTER OF JUSTICE  
MINISTRE DE LA JUSTICE  
RECEIVED - REÇU

DEC 13 2002

DEC 12 2002

HOUSE OF COMMONS  
CHAMBRE DES COMMUNES



**Guelph Police Service**

15 Wyndham Street S.  
Guelph, Ontario  
N1H 4C6  
Tel: (519) 824-1212

December 12, 2002

Justice Canada  
Lawful Access Consultation,  
Criminal Law Policy Section  
5<sup>th</sup> Floor,  
284 Wellington St.  
Ottawa, Ont. Canada K1A 0H8

Dear Minister Cauchon:

**RE: Lawful Access Consultation Document Response**

Please consider this an official and final response from the Guelph Police Service with respect to the "Lawful Access" consultation process that ends on December 16<sup>th</sup>, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Guelph Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief of Police  
Guelph Police Service

Tel: (519) 824-1212 Ext#  
Fax: (519) 822-0949

@police.guelph.on.ca

s.19(1)

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 13 2:51 PM  
To: 'la-al@justice.gc.ca'  
Cc: [REDACTED]  
Subject: Comments from OTA RE Lawful Access Consultation Document



Lawful Access.doc

Please find attached hereto an electronic version of the comments from the Ontario Telecommunications Association (OTA) regarding the Lawful Access - Consultation Document of August 25, 2002

[REDACTED]  
[REDACTED]  
Ontario Telecommunications Association  
Tel 519-773-1237 Fax 519-765-3217  
Email [REDACTED]

\*\*\*\*\*  
\*\*\*\*\*

This E-mail contains legally privileged and confidential information intended only for the individual or entity named in the message. If the reader of this message is not the intended recipient, or the agent responsible to deliver it to the intended recipient, you are hereby notified that any review, dissemination, distribution or copying of this communication is prohibited. If this message was received in error, please  
1. Advise us by reply E-mail and delete the original message.





December 12, 2002

"Lawful Access" Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

**Re: "Lawful Access" and the Small Incumbent Local Exchange Carriers  
represented by the Ontario Telecommunications Association (OTA)**

The OTA represents 19 small incumbent local telephone exchange carriers in the Province of Ontario. These companies, identified in Appendix 1 and hereafter referred to as "OTA" or "the Companies", are truly small carriers in that they serve as few as 600 network access services in the smallest and the largest being 21,445 network access services. Even the largest Company serves four distinct regions of the Province of Ontario and each region is served by its own host telephone switch. Most of the Companies, in addition to local telephony service, provide internet access and one also provides cellular services.

The Companies have a long history of close co-operation with law enforcement agencies and fully support the need to ensure continued public safety in the context of new technologies but always in delicate balance with the need to protect the privacy and rights of our customers. Due to the very vague and preliminary nature of the discussion paper, OTA finds it difficult to provide meaningful comment on the Consultation Document other than to raise 1 concerns regarding the potential financial impact on our Companies. Indeed, there are a number of issues regarding potential investment in infrastructure and administration systems contained within the Consultation document that cause grave concern to the Companies of OTA.

***First and foremost of concern to the OTA, is the discussion surrounding Costs of Ensuring Intercept Capability.***

The Companies, regardless of their size, each must maintain a host switch to provide services and several Companies must maintain additional host switches due to the

geographic separation of their serving territories. The cost to provide "Lawful Access" capability for both new technologies and services as well as when significant upgrades are undertaken could cause real and lasting financial harm to these small service providers. Even the ongoing maintenance costs and upgrade costs of the networks to maintain access capability that are likely to be forced upon these Companies by equipment suppliers could be overly onerous for such small carriers. The possibility of forbearance, as outlined in the Consultation Document, could perhaps be used to ensure these companies are not financially jeopardized but that could easily result in the undesirable creation of known safe havens within the areas served by these small providers for the criminal element. To ensure uniformity of "Lawful Access" capability across the country without causing real harm to these small Companies, and the many other small Canadian service providers, the costs of implementing this capability must be funded on a much broader base and not borne by the individual service provider. In many cases the need for this technology is driven, not so much by the small offender and petty criminal element, but by highly organized criminal organizations. The cost of implementing "Lawful Access" capability might better be borne from funds seized by the Crown from the proceeds of this organized and sophisticated criminal activity as is now permitted under various Canadian laws. If not funded entirely from this source, general public funds should be used to implement and maintain "Lawful Access" services to protect the small service providers from this unfair economic burden.

The potential costs of implementing and maintaining records and systems to support "Lawful Access" that are not currently used by the Companies is also of grave concern to the OTA whether such systems are for telephony, internet or wireless service networks. The ongoing costs to provide and store production orders, data preservation orders, data retention orders etc. as outlined in the Consultation document should be supported from external funds rather than at the sole cost of the Companies.

The OTA is also concerned that unreasonable timeframes may be imposed on the Companies to implement and operate new "Lawful Access" provisions. Reasonable timelines for providing information, for maintaining records etc. must be established with the financial and other resource limitations of the smaller carriers in mind.

Finally, the OTA notes that we were invited by way of a letter of June 27, 2002 from Michael Binder to an Industry Canada sponsored round table consultation meeting in Ottawa to discuss "Lawful Access" issues as they impact carriers. The meeting date was cancelled on very short notice and then rescheduled on even shorter notice (invitation sent to OTA September 17<sup>th</sup> for September 19<sup>th</sup> meeting) to the extent that OTA was unable to attend and present our views and concerns regarding "Lawful Access". This is unfortunate but not entirely atypical of the lack of sensitivity and acknowledgement of the breadth and scope of the telecommunications industry in Canada by higher levels of government. There are many service providers beyond the large national and regional carriers (former Stentor telephone Companies). Some of the proposals put forward in this Consultation Document, will have far more impact on these small providers than they will for the more commonly recognized and better understood large carriers. Indeed,

implementation of the costing proposals in the Consultation Document could cause serious and irreparable financial harm on the small carriers in Canada.

In closing, the OTA again stresses that it is imperative that the small service providers in Canada, including the Companies represented herein, are not burdened with the cost of implementing and maintaining "Lawful Access" systems and processes beyond what exists today. This financial burden must be borne by a much broader base than the service providers. The OTA would be pleased to provide additional information on this most important subject if requested. Please contact me at 519-773-1237 or [REDACTED] at 613-239-0610 extension [REDACTED]

Yours truly,

s.19(1)

[REDACTED]  
OTA

## Appendix 1

Amtelecom Inc.  
Brooke Telecom Co-operative Limited  
Execulink Telecom Inc.  
Gosfield North Communications Co-operative Limited  
Hay Communications Co-operative Limited  
Huron Telecommunications Co-operative Limited  
The Lansdowne Rural Telephone Company Ltd.  
Mornington Communications Co-operative Limited  
Nexicom Telecommunications Inc.  
Nexicom Telephones Inc.  
North Frontenac Telephone Corporation Ltd.  
North Renfrew Telephone Company Ltd.  
People's Telephone Co. of Forest Inc.  
Public Utilities Commission of the Corporation of the Town of Cochrane  
Quadro Communications Co-operative Inc.  
Roxborough Telephone Company Limited  
Tuckersmith Communications Co-operative Limited  
Westport Telephone Company Ltd.  
Wightman Telecom Ltd.

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)

**Sent:** 2002 Dec 13 12:06 PM

**To:** la-al@justice.gc.ca

**Cc:** cacp@cacp.ca

**Subject:** Lawful Access

Attached is correspondence from [REDACTED] of Waterloo Regional Police Service.

2002-12-18

000322

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 13 10:00 AM  
To: la-al@justice.gc.ca  
Subject: Re: lawful access

It is all very well and good to try and secure the internet.  
(all those hackers drive me nuts too!) But be aware that  
under the new IPv6 protocol there will be  $2^{128}$   
( $\sim 3.4 \times 10^{28}$ ) addresses to monitor.  
That is:  
~34,000,000,000,000,000,000,000,000,000  
addresses!

Note that the majority of these addresses will be "smart home"  
devices and that you will be monitoring stuff like when the  
bread machine comes on, or the coffee maker ... whatever!  
Also be aware that a properly equipped hacker can masquerade  
as any IP address they wish (IPv4 or IPv6). So you might  
very well end up trying to arrest someone's "smart doorbell".

I believe you will need to commission Cray to produce something  
even more powerful than their latest Fluorine cooled wonders!  
I hope the Canadian taxpayer will be able to support such efforts.  
In order to effectively monitor the internet I am confident that you  
will need a budget larger than our current defence budget! How  
likely is that to happen?

Advanced operating systems of today can encrypt ALL network  
activity at very high levels. The supercomputing budget to decrypt  
such data would likely need to be larger than the AMERICAN  
defence budget! If this monitoring is implemented you will find  
that most of the data on the internet will then be encrypted.  
Wireless networking technology is growing by leaps and bounds  
and will surely foil any attempts to control the internet.  
(Re: encryption in Canada : see the OpenBSD website -  
It would be shame to have to shut them down)

I suggest you carefully examine the relationship between Microsoft  
and the american department of justice. The american department  
of justice is always two steps behind Microsoft. They can legislate  
and prosecute all they like but will never be able to control the  
technology because they will never fully understand it, and  
Microsoft can afford to re-write their product every few years  
anyway.

With regard to trying to control Proprietary Operating Systems:  
The other possibility to effectively control the internet would  
be to make the ONLY LEGAL operating system the Open  
Source Project - OpenBSD (with encryption tech stripped  
of course)

I am sure that the only way yo control the internet is to ban it!  
Yes, you heard me, ban it altogether. Shut down the whole  
works, that is your only hope.

Actually, I just had an idea! The canadian justice deparment MIGHT  
be able to control the internet if it could hire these same hackers to  
produce viruses and worms that control the web. (or destroy it).  
This would be much more cost effective than actually monitoring.

I would also like to comment that if this type of legislation passes  
I will simply cancel my internet account and that a large number

Pierlot, Paul

---

From: [REDACTED] s.19(1)

Sent: 2002 Dec 13 1:47 PM

To: la-al@justice.gc.ca

Subject: Lawful Access question

Hello,

Can you advise if submissions can be submitted in confidence? We understand that industry associations representing many organizations will submit comments. Yahoo Canada does not belong to any of these associations, and as such we prefer to submit in confidence.

Thanks,

[REDACTED]  
Yahoo Canada Co.

Toronto, ON [REDACTED]  
[REDACTED]

Yahoo Canada <http://www.yahoo.ca/>

Yahoo Canada en français <http://cf.yahoo.ca/>

IMPORTANT NOTICE: This message is intended only for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify Yahoo Canada immediately by email at [REDACTED]

[REDACTED] Thank you.

2002-12-18

000324



December 13, 2002

Justice Canada  
Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor,  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8.

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

Please consider this an official and final response from Waterloo Regional Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Waterloo Regional Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

Chief of Police

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

## Comments on the Lawful Access Consultation Document

Lawful Access Consultation  
Criminal Policy Section  
5<sup>th</sup> Floor,  
284 Wellington St.  
Ottawa, Ontario, Canada K1A 0H8

December 13, 2002

After reviewing the August 25, 2002 proposal put forth by Justice Canada I hereby tender outstanding issues to that proposal.

Those outstanding issues are as follows:

- Freedom of Speech
- Email message & letter
- Technology & the point of Demarcation
- Burden of Costs
- Existing Law
- Definitions
- Privacy
- Subscriber Databases

**Freedom of Speech** as enumerated in our Charter reads '*Everyone has fundamental freedoms... freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication*'.

According to Statistics Canada, less than 1% of the population is behind bars for all crimes. It would seem unnecessary and inappropriate for the balance of 99% of the public to surrender, restrict or encumber their speech by allowing any monitoring not just one but all messages of subscribers mailboxes. The criminal will move on to other avenues of communication regardless of technology and the balance of us would fear that at any time anyone for good cause or not would have access to our mail. Thus, many might feel less than free to speak. To speak freely without prejudice is a reflection of our basic freedoms. Why would the 99% give up that which they enjoy now in favour of catching a criminal who is going to commit crime whether accessing technology or the Canada Post system? Government does not make a practice of reading the mail, while I am sure they could do that. Impugning our freedom to speak opening and freely goes to heart of our freedom of speech and access to our electronic mail is simply too much to accept.

**Electronic letters** or email messages are just what they appear. Written messages either postmarked or electronically stamped by a computer does not diminish the personal privacy of that communication. Nor does it change the rights of the sender in posting or electronically transmitting such a message. A

computer marks an electronic message also known as 'email' for the same purpose of intent as any member of the public uses a postage stamp. When paying for postage one assumes that a letter will be delivered to the addressee without interruption. Ergo, an email letter is the same as a posted letter and deserves the same respect, integrity, privacy and freedom accorded under law.

**Technology at the point of demarcation** is interesting and surprising. Service providers use a vast amount of technology in order to process email messaging between subscribers. The application of technology is utilized and managed differently among the many service providers in Canada. In short, one service provider may not offer the same service as another. This is good for competition and fosters growth in the marketplace. Telephone companies are regulated and are required to produce a telephone signal to each subscriber requesting access to the PSTN(public switch telephone network). The signal must be brought to the point of demarcation. So called, as this is where public access ends. The subscriber must therefore capture the signal and incorporate that signal in privately provided telephone equipment. Neither the telephone company nor any provider of telephone equipment may enter the residence or place of business of any subscriber without permission. However, the government proposes to by-passes the point of demarcation; enter a place of business solely based on the fact that the subscriber is a service provider of email messaging. This seems highly discriminatory and singles out one type of business because their of equipment or technology. Yet, every large business in Canada owns or operates large computer systems capable of offering email-messaging services to their employees and they do. Many employees enjoy conducting business using an email address targeted to each person individually. Does the government intend to include all businesses in Canada? Does the government intend to access every business that operates email messaging regardless of where or who the point of demarcation belongs to? Clearly, this requires clarification as it is unacceptable in its present form.

**The costs** to implement filters or monitoring devices should not be a cost put upon the technology community or service providers. This monitoring is not their business but rather the business of law enforcement. Firstly, the government proposes to interrupt daily business, and then require technology to access one or more subscriber mailboxes, and then expect the service provider to bear the burden of that cost. While that may be appropriate someday it seems unfair and unreasonable to ask a for-profit business to bear costs not associated with their business, but rather someone else's. In this case, law enforcement. Just because a judge issues a search warrant doesn't mean that the recipient should absorb the cost of the execution of that warrant? This smacks of an abuse of power.

**Existing law** appears sufficient to allow law enforcement to seek any information associated with criminal acts. Broadening the scope of investigation seems unnecessary without limits. The current proposal suggests that any investigation that lacks clear purpose or substance may be nothing short of a 'fishing

) expedition'. Either the investigating agency knows what they are looking for and why, or they do not<sup>3</sup>. Expanding the investigation of criminal acts may be necessary but not to the extent of allowing that investigation to randomly search, seize, and read personal messages without limitation. Ergo, existing law meets the investigative needs for criminal investigation.

**The definition of service provider** lacks clarity. The responsibility of any service provider alluded to in the consultation document is far too general in description or focus. Not all service providers render the same services. Some due transfer data, others manage data. The consultation document fails to adequately distinguish any of these and leaves one to think that all service providers are intended to be the focus. In general, the consultation document requires more meaning to its use of terms when referring to process, organization and or individuals(see 4).

) **Privacy** is another example of intrusion upon public rights as depicted in the consultation document. The Privacy Commissioner George Radwanski commented: *the interception and monitoring of private communications is a highly intrusive activity that strikes at the heart of the right to privacy. If Canadians can no longer feel secure that their web surfing and their electronic communications are in fact private, this will mark a grave needless and unjustifiable deterioration of privacy in our country'*<sup>1</sup>. Significantly changing the powers of search goes far beyond anything done in the past. Making it easier for law enforcement doesn't make it better for Canada. It simply infringes upon the public right to privacy. I further rely on the words of Douglas J., dissenting in *United State v/ White*, supra, put it at p756: "Electronic surveillance is the greatest leveler of human privacy ever known."<sup>2</sup>

**Subscriber databases** proposed by the Canadian Association of Chiefs of Police amounts to the collection of personal information prior to the commission of an offence and constitute unjustifiable extension of police surveillance into the private domain of communications. Not only is it unnecessary, but impractical. Gathering and managing such confidential data smacks of discrimination and accusation with just cause. Simply thinking or listing someone's name doesn't make them guilty of any crime. But it does send a false positive about police power.

### Recommendation

- )
- 1) I suggest that the government re-think its intent and define exactly who and what they are after. By doing so we all would clearly feel safer and knowledgeable about the conduct of any investigation into our affairs. Defining and identifying the particular target is the focus of intent.
  - 2) Before stepping on and soiling our privacy, perhaps the government could give an example of what group or groups are violating law now. Develop

their agenda for investigating such criminals without violating the majority of the public's right to privacy. For example, the government could solicit assistance from the public or anyone who volunteers to assist with such an investigation.

- 3) The burden of cost is one the government has always had, and in the past that cost was part of budgeting. I suggest that the government estimate that cost and appeal to Parliament for funding. A increase in government spending is the business of Parliament directly, and accounting for that is the review of every voter albeit Canadian. Perhaps offer a subsidy to technologists who want to work for the government in developing tools for investigation in the same way subsidies were offered to medical students who would practice in remote areas of the country.
- 4) Promote legislation that clearly identifies a crime against existing statute not an afterthought or one that hasn't been committed. Be prepared and develop alternatives. If one methodology doesn't fit or work seek others. What did we do before we had forensics? This science is the result of existing evidence that is available for further diagnostics and analysis.
- 5) Establish legal procedures that have been tested in the courts and seek to enhance those. Lowering the threshold of priority affects all information without consideration to the priority or privacy of that information.
- 6) Any assault on our basic Freedoms cannot be tolerated unless we remain silent. In that event we deserve what we get. Our ancestors fought wars to preserve our freedom. Lowering our standards demeans their sacrifice. Our mission should be to carry on the struggle to preserve our rights and seek lawful, just and fair ways to punish those who would deprive anyone of his or her right to live in a free and open society. Government serves the people at the will of the people. Not the other way around. If the any investigative practice is reasonable in private then it should stand the test of public scrutiny. If it fails then that is will of the people not the will of law enforcement<sup>(see 5)</sup>.

Respectfully,

s.19(1)

West Vancouver, BC V7T 2X9

### References

- 1) November 25, 2002 Privacy Commissioner of Canada, George Radwanski, printed on the website ...letter to the Minister of Justice, [privcom.gc.ca/media/le\\_e.asp](http://privcom.gc.ca/media/le_e.asp)
- 2) Reported in R.v Duarte
- 3) As reported in 'How Canadians Govern Themselves' 4<sup>th</sup> Edition, Library of Parliament, Senator Eugene Forsey.
- 4) THE FUTURE OF LAW IN CANADA, The Department of Justice Canada, Last Updated: 2002-06-26, Important Notices.
- 5) THE FUTURE OF LAW IN CANADA, The Department of Justice Canada, Last Updated: 2002-06-26, Important Notices.



US Internet Service Provider Association

1330 Connecticut Avenue, N.W. ♦ Washington, DC 20036 ♦ 202.862.3816 (v) ♦ 202.261.0604 (f)

December 13, 2002

The Honorable Martin Cauchon, P.C. M.P.  
Minister of Justice and Attorney General  
Department of Justice Canada  
284 Wellington Street  
Ottawa, Ontario K1A 0N2  
Canada

Dear Minister Cauchon:

I'm writing on behalf of the US Internet Service Provider Association (US ISPA), a trade association representing large Internet Service Providers (ISPs), many of which serve customers in Canada. Our members include America Online, Teleglobe, Cable & Wireless, EarthLink, eBay, SBC Communications, Verizon Online, and WorldCom. We write to request that a more detailed version of the Department of Justice's proposed "Lawful Access – Consultation Document" be made available to interested parties. Without the draft legislation and accompanying regulation, US ISPA is not able to provide you with detailed comments on the possible financial and operational effects the proposed legislation may have on the industry.

Last month, the Department of Justice met with some of our member companies and the Canadian ISP industry to unveil and discuss new surveillance proposals outlined in "Lawful Access – Consultation Document." We very much appreciate this effort to reach out to the ISP industry and to establish an open dialogue on the ideas in your consultation paper. Unfortunately, the broad concepts in the "Lawful Access" document do not provide enough details on the specific language and breadth of the regulation to allow us to develop a constructive and comprehensive response. The paper does, however, raise significant questions on how standards will be developed, how the law will be implemented, who will pay for the implementation, and whether or not certain agenda items are technically feasible. The document also leaves critical concepts too vague and ill-defined to interpret. For instance, it is entirely unclear what constitutes a "significant upgrade" and whether such an upgrade would require an ISP to make its entire network compliant or only those portions which are upgraded.

It is critical that the ISP industry and the Department of Justice work closely together to understand the costs and unintended consequences associated with this proposed legislation. US ISPA fears that some of the proposals may decrease incentives for technological innovation and competitive advantage in Canada. We understand this is not your intent. On the contrary, in

The Honorable Martin Cauchon, P.C. M.P.  
December 13, 2002  
Page 2

the consultation document you state that your intent is to create a balance between law enforcement's lawful access and the preservation of privacy, as well as ensuring "that no competitive disadvantages are placed on the Canadian industry and that the solutions adopted do not place an unreasonable burden on the Canadian public." If these proposals are not examined in further detail, the Canadian ISP industry and the public may experience the same burdens found in other countries that have passed similar legislation.

In 1998, the Netherlands enacted extensive interception proposals similar to the ones now being proposed in the "Lawful Access" document. To comply with the law, the Netherlands' ISP industry had to invest 100 million Euros in interception technology. This enormous cost, according to remarks by the chairman of Netherlands Internet Providers at a recent Electronic Commerce Forum (ECO), was passed onto the customers and partly explains the high telecommunications end-user prices in the Netherlands compared to other European countries.

Similarly, the United States in 1994 enacted the Communication Assistance for Law Enforcement Act (CALEA), a law requiring telecommunications providers to configure their systems to allow law enforcement various kinds of access to customer information. Although CALEA did not apply to the ISP industry, it is almost identical to most of the provisions in Canada's "Lawful Access" proposal, and it has cost the telecommunications industry billions of dollars over the past 8 years.

According to the 1999 Third Report and Order on CALEA filed by the US Federal Communications Commission (FCC), the Cellular Telecommunications Industry Association (CTIA) estimated that coming into interim compliance with CALEA cost the wireless phone industry in excess of US\$ 4 billion for all carriers. The report also cites the Personal Communications Industry Association's (PCIA) estimate that the nationwide cost to local exchange carriers of implementing the interim standard would be US\$ 1.73 billion. In addition, five manufacturers of telecommunications equipment offered support for these estimates by reporting that their anticipated revenues from selling software to meet CALEA's requirements would exceed US\$ 1 billion.

An April 2002 FCC Order reflects an estimate by the United States Telecom Association that the total cost of CALEA compliance would "far exceed the \$500 million appropriated by Congress to reimburse carriers for CALEA compliance." Indeed, the FCC Order cites BellSouth Corporation's estimate that implementing just six "add-on" items (called the "punch list") would cost the company between US\$ 193 and US\$ 286 million.

According to the Canadian consultation proposal, ISPs will not be reimbursed for making upgrades and new technologies compatible with government standards. This means that intercept capabilities will become a kind of government-mandated tax on technical innovation. Before upgrading equipment, the Canadian ISP industry will have to add intercept costs to the cost of the upgrade and pass them all on to the consumer. The cost of technological innovation for the ISP industry will be much higher in Canada compared to other countries, thereby diminishing Canada's competitive advantage. If not examined further, the "Lawful Access"



The Honorable Martin Cauchon, P.C. M.P.  
December 13, 2002  
Page 3

proposal provides a strong disincentive for technological innovation and investment in Canadian ISPs.

For these reasons, we request that the draft legislation and accompanying regulations be made available for a full and complete public review and that sufficient time be provided for interested parties to assess their impact and submit comments.

Respectfully submitted,

s.19(1)



US Internet Service Provider Association



# HALTON REGIONAL POLICE SERVICE

*"Progress Through Participation"*

December 13, 2002

*Trust &  
Respect*

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
284 Wellington Street, 5th Floor  
Ottawa, ON  
K1A 0H8

*Integrity*

Dear Minister Cauchon:

**Re: Lawful Access Consultation Document Response**

*Accountability*

Please consider this an official and final response from the Halton Regional Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

*Excellence*

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Halton Regional Police Service agrees and supports the submission in whole.

Sincerely,

s.19(1)

*Teamwork*

CHIEF OF POLICE

cc: Honourable Wayne Easter  
Solicitor General of Canada

*Justice*

Honourable Allan Rock  
Minister of Industry

EAN G. ALGAR, CHIEF OF POLICE

1151 Bronte Road, P.O. Box 2700, Oakville, Ontario, Canada L6J 5C7  
PHONE: (905) 825-4777/878-5511 FAX: (905) 825-9416 www.hrps.on.ca 000334



Royal  
Canadian  
Mounted  
Police

Gendarmerie  
royale  
du  
Canada

NCO In Charge  
Red Deer Special "T" Section

Date: December 13, 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5th Floor  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

Dear Minister Cauchon:

**RE: Lawful Access Consultation Document Response**

Please consider this an official response from the RCMP Red Deer Special "T" Section, "K" Division, Alberta with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

Lawful access is an extremely important and necessary tool employed in the investigation of serious crimes. Complex technologies are constantly challenging conventional lawful access methods. Criminals and terrorists are continually taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must continue to evolve and adapt so that law enforcement and national security agencies can effectively investigate criminal activities. These activities include terrorist acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, all communications service providers are not required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper and sometimes stall investigations. There are cases where persons involved in illegal activities are aware of this and take full advantage of this investigative weakness. I am aware of the additional costs attached to companies developing solutions for LEA compliance but the alternative is far more costly for Canadians. As good cooperate citizens providing a service to Canadian residences they must do their part to promote a safe and secure environment where some elements in the community are not given an unfair advantage. New companies entering the market place in Canada must be aware of their lawful access obligations when they first open for business, I feel the initial costs would be far less than having to implement

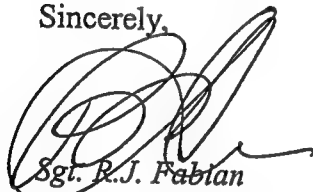
Continued RE: Lawful Access Consultation Document Response

solutions after the fact. There are many arguments against this philosophy but simply put the more freedom the criminal element has the more it cost everyone. We have long established laws to protect Canadian citizens while investigating serious criminal activity and I feel that it must be made a cooperate responsibility to comply with the needs of law enforcement.

I believe it is of the paramount that all service providers in Canada be required by legislation to ensure their public systems have the technical capability to provide lawful access to law enforcement and national security agencies. When a court order is served on any telecommunications company in Canada they must under law provide what is requested in the order as to the search and seizure of data.

I support the Government of Canada's review of current lawful access legislation and its efforts to ensure that the laws respecting lawful access keep pace with evolving communications technologies. I with my colleagues look forward to any opportunity to continue discussions on this issue as the lawful access legislative review progresses.

Sincerely,



*Sgt. R.J. Fabian*  
NCO i/c Red Deer  
Special "I" Unit  
"K" Division in the  
Province of Alberta

CC Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

Canada

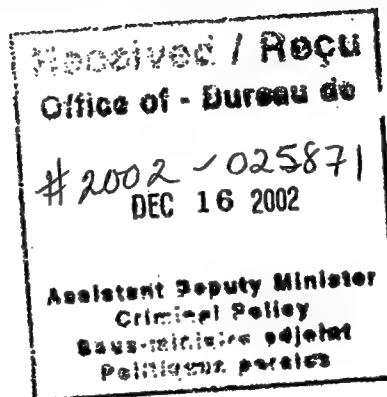
Chief of Police  
Chef de police



190 rue Brady Street  
Sudbury, Ontario  
P3E 1C7

*L. Anger*

December 13, 2002



Emergency 911 urgence

Tel/tél: Administration  
705.675.9171

Fax: Administration  
705.674.7090

Fax: Operations/  
Opérations  
705.675.8871

[www.police.sudbury.on.ca](http://www.police.sudbury.on.ca)

Address all  
correspondence to the  
Chief of Police

Prière d'adresser toute  
correspondance au  
Chef de police

Justice Canada,  
Lawful Access Consultation,  
Criminal Law Policy Section,  
284 Wellington St., 5<sup>th</sup> Floor,  
Ottawa Ontario,  
K1A 0H8

Minister Cauchon:

**RE:      LAWFUL ACCESS CONSULTATION DOCUMENT RESPONSE**

Please consider this an official and final response from the Greater Sudbury Police Service with respect to the "Lawful Access" consultation process that concludes on December 16, w002.

We have had an opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Greater Sudbury Police Service agrees and supports the submission in its entirety.

Yours truly,

[Redacted signature]

s.19(1)

Chief of Police  
/lch

cc: Honourable Wayne Easter,  
Solicitor General of Canada

Honourable Allan Rock,  
Minister of Industry



# Durham Regional Police Service

• [Redacted] Chief of Police • [Redacted] Deputy Chief • [Redacted] Deputy Chief

Friday, December 13, 2002

Justice Canada  
Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor, 284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8

Dear Minister Cauchon:

## Re: Lawful Access Consultation Document Response

Please consider this an official and final response from Durham Regional Police with respect to the "Lawful Access" consultation process that ends on December 16, 2002. We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Durham Regional Police agrees and supports the submission in whole.

Sincerely,

s.19(1)

[Redacted Signature]  
Chief of Police  
Durham Regional Police

C.C. Honourable Wayne Easter  
Solicitor General of Canada  
Honourable Allan Rock  
Minister of Industry



Royal  
Canadian  
Mounted  
Police

Gendarmerie  
royale  
du  
Canada

Technical Investigation Services Branch  
1426 St-Joseph Blvd  
Gloucester, ON  
K1A 0R2

702-025665  
CP&CT-CLP

Security Classification/Designation  
Classification/désignation sécuritaire

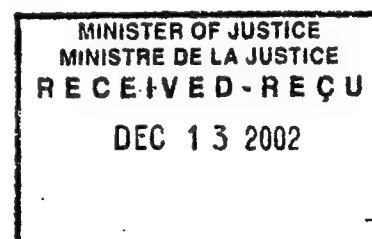
Protected "A"

Your File Votre référence

150027

Our File Notre référence

Justice Canada  
Lawful Access Consultation, Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, ON K1A 0H8



Dear Minister Cauchon;

**Re: Lawful Access Consultation Document Response**

Please consider this an official response from the HQ RCMP Special "T" in Ottawa, Ontario in respect to the "Lawful Access" consultation process that ends on December 16, 2002.

Lawful access is an extremely important and useful tool that is employed in the investigation of serious crimes. Complex technologies are increasingly challenging conventional lawful access methods. Criminals and terrorists are taking advantage of new technologies to assist them in carrying out illicit activities that threaten the safety and security of Canadians. To overcome these challenges, legislative tools must evolve so that law enforcement and national security agencies can effectively investigate criminal activities, including terrorist acts, while ensuring that Canadians' privacy and civil liberties are maintained.

Under the current laws, not all service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, the lack of a technical solution, or a delay in the ability to use it, can hamper investigations or the prevention of serious crimes or threats to national security.

To address this issue, we believe it is of the utmost importance that all service providers in Canada be required to ensure their systems have the technical capability to provide lawful access to law enforcement and national security agencies when the agencies are legally authorized to intercept a communication or search and seize data.

.../2

P.O. BOX 3070  
200 MAPLE GROVE ROAD  
CAMBRIDGE, ONTARIO N3H 5M1

TELEPHONES:  
KITCHENER, CAMBRIDGE  
& WATERLOO (519) 653-7700  
ALL OTHER AREAS (519) 570-3000  
FACSIMILE (519) 650-1793

# WATERLOO REGIONAL POLICE



Address all correspondence To: [REDACTED] CHIEF OF POLICE
--

Attention:

December 13, 2002

## OFFICE OF THE CHIEF OF POLICE

Justice Canada  
Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor,  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8.

Dear Minister Cauchon:

### Re: Lawful Access Consultation Document Response

Please consider this an official and final response from Waterloo Regional Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Waterloo Regional Police Service agrees and supports the submission in whole.

Sincerely,

[REDACTED]

s.19(1)

Chief of Police

C.C. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry



**Pierlot, Paul**

---

s.19(1)

**From:** [REDACTED]  
**Sent:** 2002 Dec 13 3:01 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Submission for Lawful Access Consultation



Untitled Attachment



iicuoofm\_jawful.pdf

**Pierlot, Paul**

---

Dear Department of Justice,

Please find attached our final report in regards to your request for commentary regarding docket "Lawful Access - Consultation Document", dated August 25th 2002.

If you require anything further please do not hesitate to contact us.

Seasons Greetings,

s.19(1)

---



Internet Innovation Centre  
University of Manitoba



Engineering  
Bldg  
[www.iic.umanitoba.ca](http://www.iic.umanitoba.ca)

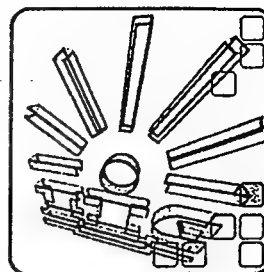
**Lawful Access Consultation**  
**Criminal Law Policy Section**  
5<sup>th</sup> Floor, 284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

December 12, 2002

**Internet Innovation Centre**

462 Engineering Bldg.  
Faculty of Engineering  
University of Manitoba  
Winnipeg, Manitoba  
R3T 5V6

(204) 474.9517 (tel)  
(204) 261.4639 (fax)  
[www.iic.umanitoba.ca](http://www.iic.umanitoba.ca)



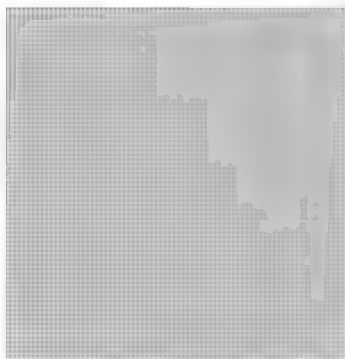
Dear Department of Justice,

Please find enclosed our commentary to your Lawful Access – Consultation Document, dated August 25<sup>th</sup>, 2002. The Internet Law Group is a collaborative effort between the Faculty of Law and the Internet Innovation Centre at the University of Manitoba.

For several months now our students' have debated your considerations faithfully and today we are pleased to submit to you our final report.

If you have any further questions about our report please do not hesitate to contact us directly at the above address.

Warmest regards,



Internet Innovation Centre

s.19(1)



# **Commentaries on Lawful Access in Canada**

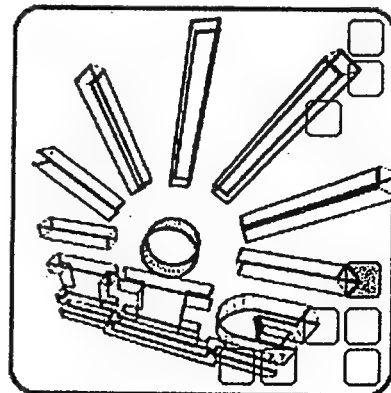
Internet Innovation Centre – Internet Law Group

(University of Manitoba)

Prepared for:

**The Department of Justice  
Industry Canada  
Solicitor General Canada**

December 12<sup>th</sup>, 2002



## Contents

s.19(1)

### Introduction

[REDACTED] 1

### The Convention on Cyber-Crime and the Charter of Rights and Freedoms

[REDACTED] 3

### Data Retention & Search and Seizure Provisions of the Convention on Cyber-Crime

[REDACTED] 9

### General and Specific Production Orders

[REDACTED] 16

### Information Orders and the Evidentiary Standard

[REDACTED] 24

### Data Production Orders

[REDACTED] 32

### The Legal Status of Email

[REDACTED] 36

### Lawful Access Legislation in the United States and United Kingdom

[REDACTED] 44

### The Lawful Access Consultation Document and The American Carnivore System

[REDACTED] 50

### The Dream of Safety: Should Canada Ratify The Convention on Cyber-Crime?

[REDACTED] 54

## Introduction

The Internet Innovation Centre – Internet Law Group is proud to present commentaries written by University of Manitoba law students in response to issues raised by the *Lawful Access Consultation Document* that was released on August 25<sup>th</sup>, 2002. Lawful Access is the phrase used to describe the interception of communications and the search and seizure of what would otherwise be private information in the interests of justice. There is no doubt that when used properly, lawful access is a viable and justified tool in combating crime and preserving the security of the country. The essential question now posed by Parliament through the *Lawful Access Consultation Document* is whether the rules that govern lawful access should be changed so as to meet the challenges posed by rapidly developing communication technologies through wireless and Internet services.

Any discussion of lawful access in Canada would have to begin with the Council of Europe's *Convention on Cyber-Crime*. Canada became a signatory to the Convention in August of 2002. The *Convention* has the goal of standardizing lawful access laws among signatory states in order to better fight computer-based and Internet-based crime. To ratify the *Convention*, Canada must first make amendments to the *Criminal Code* among other statutes. Therefore, we begin with commentaries from Mandy Lai and Anna Tosso who both examine how ratification of the *Convention* may come into conflict with our *Charter of Rights and Freedoms*. Following them are three essays by Kevin Burrton, Jeysa Martinez, and Maria Mitousis that deal with questions raised in the *Lawful Access Consultation Document*. Specifically, they focus on proposed changes in regards to the *Criminal Code* concerning various orders for information. Grant Davis then follows with a discussion on the treatment of email and whether or not email deserves the same protections as a private communication. The next two pieces take a look at how lawful access is dealt with in other countries. Kathleen Fotheringham examines the advantages and disadvantages of regulations in the United Kingdom and the United States. Martin Jungclaus argues that a more ideal system for Internet surveillance than the one proposed by the *Consultation Document* is the FBI's Carnivore system. Finally, we end with Mike Bodner's essay that takes a broader perspective and discusses whether the reasons behind the proposals are justifiable to begin with in an ethical sense.



While the commentaries are on a variety of topics and the authors are from a variety of backgrounds, there is a unifying theme behind them. Among all the submissions, there is a universal concern that the expansion of lawful access powers could potentially lead to abuse and the infringement of privacy and individual rights. This comes from a realization that over-reaction is just as dangerous as under-reaction. While the goals of lawful access reform are admirable, we must proceed with the utmost of caution in this most delicate area that is admittedly still subject to immense and daily change. Otherwise we stand to lose the very freedoms, rights, and respect for human dignity that our nation stands for.



## The Convention on Cyber-Crime and the Charter of Rights and Freedoms

s.19(1)

With the advancement of technology, our society in the last two decades has experienced widening business opportunities, staggering economic growth and instant global communications. At the same time, we have also seen the ingenuity of criminals committing old crimes in new and improved fashion and the development of new problems associated with the use of technology. Regrettably, the international nature and capability of modern technology has made unilateral national effort to curtail crimes committed through computers ineffective. International cooperation is needed in the area of technology crimes and the *Council of Europe Convention on Cyber Crime* is the first international response to address this cross-border characteristic of crimes committed through modern technology.<sup>1</sup> Canada signed the *Convention* on November 23, 2001 and is now in the process of ratifying the treaty. This process needs to be approached cautiously and carefully to ensure that the fundamental values Canadians hold dear, enshrined in the Canadian *Charter of Rights and Freedoms*, are safeguarded. This paper attempts to examine the *Convention* itself and in relation to the Canadian *Charter*. It is not intended to be a complete and exhaustive analysis of the *Convention*. However, we hope that it will bring attention to address values that are held dear in Canadian culture.

### Substantive Criminal Law

Articles 2 to 13 of the *Convention* call for criminalization of certain conduct in connection with modern technology. Their purpose is to harmonize domestic technology crimes among the signatory members so a universal platform can be established to enable efficient international cooperation.<sup>2</sup> Although the intention of Articles 2 to 13 is laudable, the

<sup>1</sup> The Council of Europe Convention on Cyber Crime, ETS 185, 23 XI 2001.

<sup>2</sup> Convention on Cyber Crime Explanatory Note, ETS 185, adopted Nov. 8, 2001, para. 33.





criminalization of behaviour is not a matter that should be taken lightly. The stigma of being charged and convicted of a crime places the government with the responsibility to ensure that the criminalization of the conduct is truly against public morality rather than to appease certain industries. Regulating behavioural problems is one thing; criminalizing them is another.

Illegal access, illegal interception, data interference and system interference are defined in broad terms such as "access to the whole or part of computer without right," "interception without right," and "serious hindering without right the functioning of a computer system." The language used in the Articles is so vague that it captures the smallest and most harmless of activities. For example, spyware would be captured under the phrase "access to the whole or part of computer without right". As irritating as it is to have spyware unknowingly uploaded to one's computer, does this activity warrant criminalization? What about a teenager who simply utilizes the defects in program design to access software but has not caused any harm to the software and its users? The government needs to define the scope of criminalized cyber activities and use clear and unambiguous language as opposed to the broad and vague language used in the *Convention*. Criteria such as the magnitude of the harm and intention must be employed to avoid the enactment of catchall provisions. Harm must be substantial and intent must be malicious. Without these two safeguards, the legislation would have difficulty passing the minimum impairment test under Section 1 of the Charter.<sup>3</sup>

Article 3 of the *Convention* requires the criminalization of "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system...." However, section 184 of the *Criminal Code* has made it an offence to intercept a private communication.<sup>4</sup> Private communication has been defined as any oral or telecommunication between two individuals in Canada.<sup>5</sup> Although section 184 is currently limited to oral and telecommunications, the rationale underlying its enactment remains the same. Privacy is a fundamental value highly regarded by Canadians and invasion of privacy is not an act tolerated in Canadian society. Rather than enacting an entirely new provision criminalizing the interception of non-public transmissions of computer data, section 184 should be allowed to

<sup>3</sup> *R. v. Oakes*, [1986] 1 S.C.R. 103.

<sup>4</sup> *Criminal Code*, R.S.C. 185, c. C-46.

<sup>5</sup> *Ibid*, s.163.



respond to technological changes and adapted to include communications between computers. Similarly, section 430 of the *Criminal Code* titled "Mischief" prohibits willful tampering, damaging and destruction of property and data. This section could be also adapted to deter and reprimand those cyber activities that are less harmful and are of a mischievous nature.

Throughout Articles 2 to 13, a prohibited cyber activity needs to be committed internationally before a crime is substantiated at the national level. Our government needs to be cautious in avoiding a creation of a two-tier system. A prohibited cyber activity, such as interception of private transmissions of computer data, is no more criminal in nature when it is committed through more than one country than when it is committed within Canada. If such a two-tier system is created, section 15 of the Charter would likely be infringed and section 1 would not be able to save such an infringement.

Article 6 of the *Convention* aims to prevent the rise of a black market supplying tools and devices that assist the carrying out of the offences under Articles 2 to 5.<sup>6</sup> It is understandable that the criminalization of the sources of such a supply is necessary in turn to enable effective combat of cyber crimes. To avoid over-criminalization, paragraph 1(a)(i) limits the prohibition to the supply of a device that is "designed or adapted primarily" for the purpose of committing, and "with the intent" of committing the offences under Articles 2 to 5. The government needs to exercise care in specifying the prohibited acts under Articles 2 to 5 or the purpose of paragraph 1(a)(i) will become all too feeble and be defeated.

Article 11(1) of the *Convention* stipulates the criminalization of aiding or abetting offences established under Articles 2 to 10. Liability arises for aiding or abetting where the person who commits an offence established in the Convention is aided by another person who also intends that the offence be committed.<sup>7</sup> There is no question that Article 11(1) is a broader provision than Article 6 but there will be times where Article 6 and 11(1) overlap. Person A, who supplies a computer virus which is designed primarily to attack a computer system and intends the virus to be used to attack the computer system, can also be deemed as aiding person B who releases the virus into the computer system. As a result, person A can be tried twice for the same crime

<sup>6</sup> Explanatory Note, *supra*, para. 71.

<sup>7</sup> *Ibid*, para. 119.



he had committed. Either section 21 of the *Criminal Code* would need to be modified to address the intended purposes of both Article 6 and 11(1) of the Convention, or new legislation enacted under Article 6 would need to avoid the possibility of double jeopardy.

Articles 7 and 8 of the *Convention* are in place to address the issues of computer-related forgery and fraud. Forgery and fraud are crimes as old as men have lived. Although the means of forgery and fraud are becoming harder to detect with the development of modern technology, the nature of the crimes remains the same. Sections 366 and 380 of the *Criminal Code* have already criminalized the acts of forgery and fraud. Modification of the sections would be required to ensure that the law has adapted to the progress of time and technology. An enactment of new criminal provisions relating to computer forgery and fraud would be superfluous and create two standards for the same offences. As a general matter, the law should be technologically neutral and avoid adopting separate provisions for crimes online and crimes offline.<sup>8</sup>

Furthermore, Article 7 stipulates the criminalization of suppression of computer data. According to the Explanatory Report of the *Convention*, suppression includes the holding back and concealment of computer data.<sup>9</sup> Section 366(2) of the *Criminal Code* has only made it an offence to add, alter and delete material information. Similarly, Article 8 calls for the criminalization of fraudulent acts, through the use of the computer, which result in intangible loss that has an economic value.<sup>10</sup> Section 380 of the *Criminal Code*, however, has only gone so far as making a fraudulent act an offence in regard to tangible property loss. Articles 7 and 8 have no doubt broadened the scope of the prohibited acts enumerated in sections 366(2) and 380 of the *Criminal Code*. This expansion of prohibited acts needs to be the attention of legislative debate. The focus should be on whether such expansion is necessary and in relation to section 7 of the Charter.

Article 9 of the *Convention* seeks to strengthen protective measures for children against sexual exploitation through the use of computer systems.<sup>11</sup> However, Article 9 encounters a similar

<sup>8</sup> "Trust And Security In Cyberspace: The Legal And Policy Framework for Addressing Cybercrime", A Project Of Internets And The Center For Democracy And Technology, August 2002, [www.edt.org](http://www.edt.org), p.5.

<sup>9</sup> Explanatory Note, *supra*, para. 83.

<sup>10</sup> *Ibid*, para. 88.

<sup>11</sup> *Ibid*, para. 91.



problem posed in Articles 7 and 8. Article 9(2)(c) criminalizes computer-generated images that realistically depict a minor engaging in sexual explicit conducts. Section 163.1(1) of the *Criminal Code* has not extended the meaning of child pornography to include computer-generated images. Although the purpose of Article 9(2)(c) is to prevent the seduction of children into participating in such acts and the formation of a subculture acquiescing child abuse, legislative debate is much needed in this area as it is as much a political as it is a legal issue.<sup>12</sup>

Article 10 is the last provision that addresses substantive law issues and is one of the most controversial provisions in the *Convention*. Article 10 calls for the criminalization of copyright infringement on a commercial scale and through the use of computers, pursuant to the obligations a signatory member has undertaken under other international treaties. As we have indicated earlier, the criminalization of behaviour is only warranted when the conduct is abhorrent and against public morals. Commercial disputes between two parties can rarely create such an effect. Although civil offences such as assault are not a bar to the criminal offence of assault and vice versa, the offence of assault was enacted in both civil and criminal courts for two different purposes. The civil court is primarily used to resolve the dispute between two parties while the criminal court is used exclusively to express public disapproval of immoral conduct. Commercial disputes of copyright infringement often involve complex issues such as unsettled law and economic factors. There is no certainty that every copyright infringement would appall public morals. Furthermore, it would be a waste of taxpayer's money to have issues such as whether there is copyright infringement tried twice at the federal courts, since two different standards of proof are required in civil and criminal actions.

#### Recommendations on Section I of Chapter II of the Convention

- The scope of criminalized cyber conduct must be limited to avoid the capture of harmless and economically viable activities, and avoid the possibility of double jeopardy.
- The scope of criminalized cyber conduct must be defined in clear and unambiguous language.

---

<sup>12</sup> *Ibid*, para. 102.



- The element of internationality should be carefully construed to avoid the creation of a two-tier system of crimes online and crimes offline.
- If existing legislation already addresses the concerns raised in the *Convention*, modification of the legislation rather than new enactments should be attempted.
- If the criminalized activities are broader under the *Convention* than the existing legislations, the attention of legislative debates must be brought to the expanded criminalized acts.



## Data Retention & Search and Seizure Provisions of the Convention on Cyber-Crime

s.19(1)

The Council of Europe's *Convention on Cyber-Crime*, which received international acclaim, and at the same time, international criticism, is the first international treaty to address criminal law and procedural aspects of various types of offending behaviour directed against abuses of computer systems, networks or data as well as a variety of crimes perpetrated on the internet. The European Committee on Crime Problems, an intergovernmental body reporting to the Council of Europe's Committee of Ministers, approved the final draft on June 22, 2001 and signed on November 23, 2001. The *Convention on Cyber-Crime* is the climax of a series of discussions throughout the 1990s dealing with the increasing use of the Internet as a tool to keep connected, and for some, as a tool for criminal activities. These issues supercede international boundaries and domestic laws, and it is clear that it is necessary to work together with international partners to ensure that cyber-crime is stopped.

Canada has played a formative role in the development and initial discussions of this convention through the G8 Group of Senior Experts on Transnational Organized Crime (Lyon Group), the Committee of Experts on Crime in Cyberspace of the Council of Europe (PC-CY), and the OAS Group of Government Experts. Furthermore, Canada is a non-member state of the Council of Europe and it is a signatory to this convention (November 23, 2001). However, Canada has not yet ratified the convention. Ratification would mean that Canada's laws must comply with the international convention. As it stands, being a signatory is akin to an "agreement-in-principle" but this stance does not force compliance.

I will discuss briefly the implications of specific articles dealing with data retention, data preservation orders, and spontaneous information and sharing. To keep this within a Canadian context, I will examine how the articles of the *Cyber-Crime Convention* could contravene



privacy considerations and may constitute an unreasonable search and seizure pursuant to s.8 of the *Canadian Charter of Rights and Freedoms*. In the event that Canada ratifies the *Cyber-Crime Convention*, I suggest that the following key recommendations must be implemented to ensure that our *Charter* values are protected:

### **Key Recommendations**

- Searches and data retention and storage must be specific and the individual should be made aware of such searches through a warrant issued by a person able to act judicially.
- Internet Service Providers must be legislated to inform of illegal activity, but a strict criteria must be enacted so that the search is based on reasonable grounds.
- Any material found in the search that is not under the specific search must be kept confidential to ensure the individual's rights to privacy.

### **Data Retention and Preservation Orders**

The intent of the *Cyber Crime Convention* is to breakdown traditional walls that have barred enforcement of criminal law for Internet related crimes that may cross international boundaries. However, breaking down these walls is not a clear-cut blow. Removing one barrier may impact on another area of public policy, and thus compromise rights afforded to Canadian citizens. For instance, Article 14 and Article 15 deal with the scope of procedural provisions and Article 16 complements them and deal specifically with Data Preservation Orders:

#### **Article 14 – Scope of procedural provisions**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceeding
- 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
  - a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
  - b other criminal offences committed by means of a computer system; and



- c the collection of evidence in electronic form of a criminal offence.
- 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.
- b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:
- i is being operated for the benefit of a closed group of users, and
  - ii does not employ public communications networks and is not connected with another computer system, whether public or private,
- that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

#### Article 15 – Conditions and safeguards

- 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
- 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.





- 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

#### **Article 16 – Expedited preservation of stored computer data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
- 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

The powers conferred in these sections are sweeping, but notably they apply when a specific criminal investigation is underway (Article 14). Accommodating such legislation may lead to casting of virtual fishing nets to collect and maintain data from an individual's computer. It may cover the entire computer, not just specific files, and this may be considered to be an invasion of privacy. Computers are increasingly a tool that makes us all multi-taskers and information found on our hard drive is a revealing insight into our individual interests and activities. For many, the technological progress has made us dependent on the computer as a critical tool for a variety of daily tasks, from banking to personal communications. Records of our Internet searches and our e-mail contacts are important to us, but such information is important to others as well. Much

abuse is possible, and such information can be sold for marketing purposes, as has been seen with cookies on individual computers or the selling of e-mail addresses for spamming.

The *Cyber-Crime Convention* has created a number of safeguards but they may be interpreted in many ways. For instance, “the Principle of Proportionality,” as referred to in Article 15(1) is vague, and its interpretation and implementation may vary from country to country. Article 15(2) refers to “judicial or other independent supervision” but who will be playing this role? From this small sample, it is clear that the wording of the *Cyber-Crime Convention* is loose enough for room for interpretation, but too much interpretation may occur and thus its effect is too watered down.

Another pertinent question is who will have this data retention power? Should it be the respective governments, the police, or the Internet service providers?

The United States, which has been seen as the internet’s Wild West and has embraced the “internet libertarian spirit” has implemented the *Patriot Act* which states that U.S. web users can have their surfing monitored if a judge is told that the information gleaned from the *interception* could be relevant. In many respects, this parallels the United Kingdom’s legislation found in the *Regulation of Investigatory Powers Act* of 2000. In both of these cases, the web user never needs to know that the investigators have been monitoring information, and the investigators do not have to report back to court. In this scenario, a mere suspicion can trigger the data retention request and monitoring can allow investigators to compile a picture of the individual’s movements online, with websites they have visited, nature of internet searches and records of e-mails.

### **Spontaneous Information and Sharing**

Under the U.K. and American Acts, Internet Service Providers may even “volunteer” the information to the law enforcement agencies. Such information sharing which can be done without the individual who purchased the service’s knowledge appears to be an invasion of privacy. This does not seem to be precluded under the *Cyber-Crime Convention*. In fact, Article 26, Spontaneous Information considers this scenario:



## **Article 26 – Spontaneous information**

- 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
- 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

It is important to note that the operative word here is “voluntary.” The ISP may or may not wish to comply with the *Cyber-Crime Convention*. It may be necessary to legislate compliance by ISPs to ensure that this Article would be followed.

Moreover, Article 26 leaves open the possibility that an individual's files and entire computer internet usage and e-mails can be given to a third party investigator. It does not state that the individual needs to be made aware of such an investigation. The scope of the investigation could be wide, although Article 26(1) states that it must be “concerning criminal offences.” However, with spontaneous information, the unobstructed access to anything on the computer is like casting the virtual fishing net and keeping everything found. An individual's privacy concerning whatever other information that is in the computer system is exposed.

### **S. 8 of the Charter**

The spontaneous information article is fundamentally against the Canadian Constitutional requirements under s. 8 that outlines valid search and seizure requirements. Our requirements state that where it is feasible to obtain prior authorization, it must be done, usually in the form of a warrant issued by a person able to act judicially and to assess the evidence as to whether the appropriate standard has been met in an entirely neutral and impartial matter. The warrant to search is not totally expansive or without limits. It is based on reasonable and probable grounds



and an impartial review of the suspicion. In essence, this ensures that the authorization balances a person's right to privacy with the broader rights of law enforcement and compliance with the law.

Since it is not necessary under the *Cyber-Crime Convention* to inform authorities, and it is possible to just pass information on to third parties, this article would constitute an unreasonable search and thus would be in violation of s. 8.

Furthermore, Internet searches that are capable in cyberspace mean that the individual under investigation may not even be aware of the search. Since searches can happen electronically, data can be saved, downloaded or transferred from his/her own computer without his/her knowledge. Canadian law, pursuant to s. 8, states that a person seeking to justify a warrantless search must rebut the presumption that such search is unreasonable.

The common law protections found in precedent cases such as *Hunter v. Southam* do not adequately reflect the new Internet reality.<sup>1</sup>

### Conclusion

Without specific provisions in any proposed legislation designed to implement the spirit of the *Cyber Crime Convention*, individual Canadians' rights may be violated. The convention is a progressive step forward to coordinate international law enforcement for crimes in cyberspace. However, since the internet's uses are so multifarious and continuously evolving, we must be very careful in giving such sweeping rights to an individual's digital information without balancing their right to privacy and security against unreasonable search and seizure.

---

<sup>1</sup> *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, 14 C.C.C. (3d) 97, 41 C.R. (3d) 97 (8:0).



## General and Specific Production Orders

s.19(1)

Production orders should be seen as limited extensions of the current search warrant and intercept authorization provisions in the *Criminal Code*. They may be seen as enhancing the efficiency of lawful access to information by law enforcement agencies, given the complexities of modern telecommunications networks. It is easier and less intrusive for service providers to produce intercepted information (once they have implemented the required technology to intercept the information) than it is for law enforcement officials to execute search warrants to retrieve such information. However, it is important to recognize that the benefits of production orders in these cases stem from the complex nature of the technology involved and the widespread use of this technology for unlawful purposes. There is a legitimate need to increase the ability of the state to lawfully access information in these specific circumstances. Production orders may help to serve this purpose, but their application should be limited to the scope of the proposed lawful access legislation, that is, to obtain data intercepted by a service provider under a lawful order from the court.

The primary reason in favour of limiting the application of production orders is the protection of individual privacy, as guaranteed by the Canadian *Charter of Rights and Freedoms*. The wide-ranging ability of law enforcement to obtain orders to produce information may be seen as opening the door for so-called "fishing expeditions," if not properly constrained by judicial review. In the context of the proposed lawful access legislation, it should be recognized that people are increasingly using computers as a primary means of communication, not only in respect of business transactions, but also personal transactions such as banking and shopping. There is no doubt that most users recognize that there is a risk that information sent over the Internet may be unlawfully intercepted. This is evidenced by the popularity of encryption software and the widespread use of communications via "secure" data transmission technology. All of this indicates that Internet users have a reasonable expectation that their communications



will be private. Section 8 of the *Charter* protects individuals against unreasonable search and seizure, and this protection extends to unreasonable interception of private communications. The Supreme Court of Canada applied s. 8 in *R. v. Duarte*, holding that a recording of an informant's conversation with an undercover officer constituted unreasonable search and seizure.<sup>1</sup> The undercover officer, as one of the parties to the communication, had consented to the recording, making it lawful under s. 184 of the *Criminal Code*, and therefore did not obtain judicial authorization for the interception. This lack of judicial review of the actions of the state was considered to be unreasonable for purposes of s. 8 of the *Charter*. With respect to lawful access, service providers may often intercept information in order to facilitate the transmission of the information in the course of providing their services. Such interception is lawful under s. 184 of the *Criminal Code*, however an order to produce such information may offend s. 8 of the *Charter*. Judicial review, then, will be an important procedural component of any production order.

There are many issues that arise in respect of the nature of information subject to the proposed production orders. Although the proposed legislation deals with all types of telecommunications service providers, the comments here will be restricted to the proposed production orders as they relate to Internet service providers ("ISP's"). The Lawful Access Consultation Document proposes for consideration the creation in the *Criminal Code* of a general production order and a specific production order. The purpose of these two types of orders, and the procedural safeguards that should accompany them are discussed below.

### **General Production Order**

The proposed general production order as described in the Consultation Document would require a third party custodian of documents to deliver or make available those documents to law enforcement officials within a certain time period. This definition extends beyond the scope of the object of the proposed legislation, which is concerned with ensuring lawful access to information transmitted via telecommunications networks. Consistent with the Council of

---

<sup>1</sup> *R. v. Duarte*, [1990] 1 S.C.R. 30.



Europe *Convention on Cyber-Crime*, the general production order should be directed towards the requirement to deliver intercepted *computer data* to law enforcement officials.

A general production order would facilitate lawful access to the content of communications transmitted over the Internet or by e-mail. Due to the complexity of the technology involved, and the fact that the technology is constantly changing, the individual ISP's are in a better position to provide information to law enforcement officials than are the law enforcement officials to seize the information under a traditional search warrant. It follows that a general production order would be an efficient and minimally intrusive method by which lawful access to information could be achieved. However, the nature of Internet and e-mail communications raises several issues in respect of the procedural standards that should be adopted in respect of this type of order.

Since the general production order is concerned with accessing content data from the computer system of the ISP, it would at first seem logical that it should be treated as an extension of the search warrant provision in s. 487 of the *Criminal Code*. That section already allows for lawfully authorized search and seizure of computer data contained in or available to a computer system at the location to be searched. The ISP's computer facilities would contain the data sought after, and a production order could be issued for the ISP, as custodian of the data, to produce the data under similar circumstances as a search warrant would otherwise be issued to search for and seize the data. This would mean that the standard for issuance of the production order would be reasonable grounds to believe that the information sought after is contained in the ISP's computer at the time that the order is given. Such a requirement would preclude anticipatory orders, and would also require a high degree of specificity with respect to the sought after data.

However, a production order in respect of data intercepted by an ISP could also be viewed as an extension of an authorization to intercept communication under Part VI of the *Criminal Code*. In this case, the standard would be reasonable grounds to believe that an offence has been or will be committed, and that the information produced would provide information in respect of that offence. In this case, the order could be anticipatory, allowing information to be obtained over a



specified time period. This would be more consistent with the object of the lawful access legislation.

The issue in respect of the nature of e-mail communications will be dealt with elsewhere in this document. It is enough to say here that in any event, if an ISP is ordered to produce information, it will be either stored in the ISP's computer system during the transmission process or will be intercepted in-transit (during upload or download) by the ISP by virtue of technology implemented under the proposed legislation. The production order should be viewed therefore as a tool used to give effect to a search warrant or an authorization to intercept communication, as the case may be, rather than a stand-alone order. The order would be issued once the warrant or authorization had been obtained, similar to the existing assistance order provision in s. 487.02. Implemented in this way, the production order would come under the umbrella of the current procedural safeguards and judicial review provided for both searches and interceptions. In addition to the existing safeguards, a provision should be added requiring strict confidence from the ISP delivering the information.

A major issue in respect of the production of information by an ISP is that often the information will be encrypted. The issue is more related to the types of infrastructure requirements that will be implemented under the proposed legislation to ensure lawful access to data, however it is of significance in respect of production orders because encrypted information has no evidentiary value until it is converted to plaintext. Therefore, the data to be produced must first be decrypted. There are major issues surrounding this process, many of which have been identified by the Information and Privacy Commissioner for Ontario<sup>2</sup>. In her submission to Industry Canada, the Commissioner identifies that decryption of data would require a court order, but in order to determine whether the information being intercepted fell within the scope of that order, access to the decrypted information would be required. This would require law enforcement agencies to have continuous access to the 'in-transit' information through a third party having the capability to decrypt the information. Presumably under the proposed legislation the third party would be the ISP. Without going into a detailed discussion of the issues relating to encrypted

<sup>2</sup> Ann Cavoukian, Ph.D., "A Cryptography Policy Framework for Electronic Commerce" (1998), online: <<http://www.ipc.on.ca/english/pubpres/reports/crypto.htm>> (accessed: 30 October 2002).





data, it can be seen that the proposed production order could be used to obtain private information on a preliminary basis in order to obtain the necessary grounds to obtain a warrant to intercept or seize the data. This reinforces the need to make the production order contingent on the issuance of a search warrant or intercept authorization.

In summary, the *Criminal Code* should be amended to include a provision for a general production order. This order, however, should be limited to the purpose for which it is proposed, namely facilitating access to information from telecommunications service providers. Also, there should be a provision included to require strict confidence of the party delivering the information. Finally, the order should not be a stand-alone order but should be issued only if a search warrant or authorization to intercept has been issued.

#### Specific Production Order

The Consultation Document proposes the creation of a specific production order for traffic data and other information that carries with it a low expectation of privacy. In this respect traffic data is compared with dial number recorders ("DNR's") and tracking devices, for which specific production orders already exist in the *Criminal Code*. Because of the low expectation of privacy associated with this type of information, the standard for the existing production orders is that of reasonable grounds to suspect rather than to believe that an offence has been or will be committed. It is suggested that the proposed specific production order be created following the same standard.

With respect to telephone numbers, the Ontario Court of Appeal held in *R. v. Fegan* that there is no reasonable expectation of privacy in respect of DNR information.<sup>3</sup> The DNR contained only information about what numbers had been dialed and gave no information about whether the intended recipient answered nor any information regarding the content of the communication. The Court also held that dialing a telephone number does not constitute a communication, and even if it did it would be a communication for which the recipient would be the service provider, who could give consent to the release of that information.

<sup>3</sup> *R. v. Fegan* (1993), 80 C.C.C. (3d) 356, 21 C.R. (4th) 65 (Ont. C.A.)



There are certainly similarities between traffic data and DNR information. Traffic data includes the Internet or e-mail addresses of the parties, similar to telephone numbers, for which there would be a low expectation of privacy. However, there are also differences in that traffic data also contains information that can provide some information regarding the nature of the communication to which it is attached. For instance, the size of the file and duration of communication can be obtained, which can indicate the nature of the communication. Also, the word 'attached' here is not insignificant. These are communications in progress, unlike telephone calls in which there is no communication transmitted until the recipient answers the call. It is therefore advisable to limit the definition of traffic data for purposes of production orders to data similar in nature to telephone numbers, such as Internet addresses and routing information. This would best be accomplished by amending the current provisions for telephone-related information in s. 492.2 of the *Criminal Code* to include the more limited definition of traffic data suggested above.

With respect to the proposal to create other types of specific production orders under the lower standard of suspicion, it would be possible to do so in some cases. A good example would be a specific production order for electric utility records as in *R. v. Plant*, where excessive consumption of electricity indicated the presence of a marijuana growing operation.<sup>4</sup> The Supreme Court held that these records were not of a "personal and confidential" nature and therefore were not protected by s. 8 of the *Charter*. However, in each case the determination of the confidentiality of the information is dependent on a number of factors. In *Plant*, Sopinka J. stated that the parameters of s. 8 protection should be determined "considering factors such as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming confidentiality, the place where the information was obtained, the manner in which it was obtained, and the seriousness of the crime being investigated."<sup>5</sup> Determination of confidentiality under this analysis would be on a case-by-case basis, and therefore accessing such information in each case should be subject to judicial review under the current search warrant provisions.

---

<sup>4</sup> *R. v. Plant* [1993] 3 S.C.R. 281.

<sup>5</sup> *Ibid.* at 293



Internet Innovation Centre – Internet Law Group

---

In summary, rather than creating a new provision in the *Criminal Code* for a specific production order for traffic data, the current provisions for telephone-related information in s. 492.2 should be amended to include traffic data, and traffic data should be limited to Internet and e-mail addresses and routing information. As well, the *Criminal Code* should not be amended to include provisions for specific production orders created for other cases where the expectation of privacy is low, because this must be evaluated on a case-by-case basis.



## INFORMATION ORDERS AND THE EVIDENTIARY STANDARD

 s.19(1)

### A) Orders to obtain subscriber and/or service provider information

The Lawful Access document expresses the need for the creation of a production order to deal specifically with subscriber and/or service provider of information for the purposes of facilitating law enforcement agencies with the powers they need to deal with crimes in the context of new technologies. The document explains the concern that, although the *Criminal Code* already provides for production/collection orders, these provisions in the *Criminal Code* are too narrow and hence the argument being made is that more is needed to obtain information at the early stages of an investigation. The reasoning provided in this document as to why we should work towards incorporating these orders into our legal system is to remove the barriers that exist for the purposes of facilitating and expediting the information collection process. In effect, this means that the goal of the suggested changes is to bypass the need to have a cooperative custodian of the information and to operate without the need of a court order.

Along this line of justification the document mentions a further impediment in the current system, that being that in some circumstances law enforcement agencies are not able to obtain a warrant under the *Criminal Code* because the information being sought is required either for non-investigatory purposes or because they are at the early stages of an investigation.

The document gives the impression that, without the creation and incorporation of these orders into the *Criminal Code*, law enforcement agencies will not be able to operate and function effectively in society. This is clearly far from accurate. It has always been the case that law enforcement officials have operated with some restrictions as to what they can and cannot do at certain stages of an investigation. These restrictions have long been in place for the purposes of



maintaining a balance between the rights of the individuals to be left alone with that of the rights of the state to intrude on privacy in the furtherance of its goals; namely, the need to combat crime. However, it is clear that law enforcement agencies have operated effectively and continue to do so within these legal parameters. Amongst the reasons provided to justify the need to have the creation of these orders is the notion that citizens of this society do not expect that there is much privacy in their communications via electronic means. Since it is assumed that this is the general standard accepted by Canadians, the document seems to reinforce the notion that providing the police with these extra powers would not be considered as a grave intrusion into our privacy. The document also rationalizes the need to incorporate these changes into our laws because it emphasizes that the area it is dealing with concerns new technology and hence it has not been adequately addressed in the *Criminal Code*. The reality is that the proposed orders would increase police powers and, if the requirement to obtain a warrant is removed (in order to facilitate or/and expedite the process), it is bound to bring with it dangerous implications and this should be of great concern to all members of our democratic society.

The order, as proposed, undermines the expectations of privacy of all those who value their privacy in their use of electronic communication devices. In fact, it is a frightening thought to think that law enforcement officers could make use of these investigatory tools without a warrant, mainly because it would do away with the responsibility that law enforcement officers have to citizens. Absent the courts' involvement in the assessment of private information, there would be no restraint and hence police could employ these tools without any limits. This approach would be contrary to every reasonable expectation that most people in our democratic society have.

The courts have been charged with the role of determining whether an intrusion of privacy by the police is justified. If the modifications to the *Criminal Code* are made without the requirement of the involvement of a judicial body, the police would be free to determine when they would act, and this would lead them to exercise an unlimited amount of discretion in defining the scope of their intrusion. Hence, the involvement of the courts as the judicial body is a component that should be given great weight and consideration as they stand as the guardians of the laws and are there to ensure that the constitutional principles protecting privacy interests are not ignored.



**B) What evidentiary standard should be required for production orders?**

As suggested above, if any changes are to be made, the evidentiary standard should be ultimately determined by the courts. It is suggested in the document that obtaining authorization from the courts can be an impediment to an investigation (hence one of the reasons supporting the implementation of these orders). However, if we are to explore what is required from a police officer to obtain a court order/warrant one can reasonably conclude that the *Criminal Code* need not undergo such extensive and broad amendments as is being suggested. The needs of the police can be met by simply making small modifications with respect to the access to new technology. To support the above statement we should consider what is currently required from the police to comply with the current laws in order to collect the information sought. The police are required to provide the court with an affidavit, the contents of which will be considered and, if the judge is satisfied, an order will be granted.

The evidence required by a judge in the said affidavit prior to issuing a court order should be examined in the context of current case law in order to assess whether or not the recommendations being proposed, when compared to the current steps, would provide the police with fewer obstacles in obtaining the information required in their battle against crime.

In a recent decision by the Supreme Court of Canada, *R. v. Araujo*, although dealing with the issue of wiretapping, the court stated that:

Looking at matters practically in order to learn from this case for the future, what kind of affidavit should the police submit in order to seek permission to use wiretapping?

The legal obligation on anyone ... is a full and frank disclosure of material facts...All that it must do is set out the facts fully and frankly for the authorizing judge in order that he or she can make an assessment of whether these rise to the standard required in the legal test for the authorization. Ideally, an affidavit should be not only full and frank but also clear and concise. It need not include every minute detail of the police investigation over a number of months and even of years.



Recent jurisprudence has confirmed that such language is to be interpreted in a practical commonsense fashion, so that courts may issue wiretap orders even when government has not pursued all other investigative techniques.<sup>1</sup>

The requirements of the affidavit seem very straight forward. In the absence of the requirements above, anything less should cause serious concerns when one considers the need to maintain a balance between legitimate search/collection of information and the need for respect of privacy and of unwarranted intrusion. In *R. v. Duarte*, it was held that “the assessment of the constitutionality of a search and seizure must focus on its ‘reasonable’ or ‘unreasonable’ impact on the subject of the search or the seizure, and not simply on its rationality in furthering some government objective”.<sup>2</sup>

It is also important to acknowledge that, despite not having the suggested changes implemented in our *Criminal Code*, Canadian jurisprudence has given wide interpretation to sections that require it. This approach is well reflected in *R. v. Hiscock* in regards to s. 186(1):

...s. 186 does not require that all alternative investigative techniques have been tried. It is not simply a recourse of last resort. It is a technique which must not be used in the absence of serious, probable grounds, but which can be employed not only when the other methods have failed, but also, when they appear to have little chance of success or when the urgency of the matter would otherwise render the investigation unsuccessful.<sup>3</sup>  
[Emphasis added.]

#### Reasonable Expectations of Privacy

In considering amendments for the issuance of production orders of subscribers in order for law enforcement officials to have easier access to obtain information expediently, it is important to note that the courts have also established that the test to be applied is not that which would be the “most efficacious” approach of investigation/collection of information, but rather the test should follow a standard of “investigative necessity requirement,” as presented in *R. v. Araujo*:

The meaning of the investigative necessity requirement is of critical importance by reason of the conflict between the privacy interest involved in

<sup>1</sup> *R. v. Araujo*, [2002] 2 S.R.C. 992.

<sup>2</sup> *R. v. Duarte*, [1990] 1 S.C.R. 30.

<sup>3</sup> *R. v. Hiscock*, [1993] 1 S.C.C. 325.



wiretapping operations and the needs of law enforcement agencies in their difficult fight against some forms of sophisticated and dangerous criminality...Indeed, in the end, one might well argue using such an efficiency standard, that wiretapping should always be available to the police, since it might often help catch more criminals. Such a result would rightly send a chill down the spine of every freedom-loving Canadian.<sup>4</sup>

It is clear from this examination that courts also express concerns with respect to the privacy considerations of individuals as they relate to basic but essential rights of all members in our society. Therefore, the need by the law enforcement officials to have access to information has to be balanced with the need to protect the privacy rights of citizens in our society.

#### Charter of Rights and Freedoms - Section 8

It should be clear to all, after much case law on the matter, that s. 8 of the *Charter* was designed to provide continuing protection against unreasonable search and seizure and to keep pace with emerging technological development. It is difficult to put into place the amendments to the *Criminal Code* as suggested in the document without infringing on this basic right. In *R. v. Duarte* the court held that unauthorized electronic audio surveillance was a violation of s. 8 of the *Charter*.<sup>5</sup> In *R. v. Wong*, the Supreme Court of Canada made reference to *Duarte* and stated that "privacy would be inadequately protected if an assessment of the reasonableness of a given expectation of privacy were made to rest on that consideration whether the person concerned had considered the risk of electronic surveillance."<sup>6</sup> Basically, the court stated that the expectation of privacy should be measured/considered by the standards of privacy that a person can expect to enjoy in a free and democratic society. The court in *R. v. Wong* went further to say that "...the agents of the state were bound to conform to the requirements of the *Charter* when affecting the intrusion in question." While considering the examination of these issues of privacy in light of new challenges posed by new technology (as indicated in the document), the Supreme Court of Canada upheld in *R. v. Duarte* that "It would be wrong to limit the implications of that decision to a particular technology." Reaffirmed in *R. v. Wong*, "rather the court said in *Duarte* that it must be held to embrace all existing means by which the agencies of the state can electronically

<sup>4</sup> *R. v. Araujo*, *supra* at 11.

<sup>5</sup> *R. v. Duarte*, *supra* at 30.

<sup>6</sup> *R. v. Wong*, [1990] 3 S.C.R. 36





intrude on the privacy of the individual, and any means which technology places at the disposal of the law enforcement authorities in the future.” Therefore, much consideration and thought should be given to the *Charter* rights in the context of the suggested amendments as these suggestions would be clearly considered as being intrusive on the rights of the individual.

Also, greater weight than is given to *The Personal Information Protection and Electronic Documents Act* should be noted as this Act provides the governmental authorities with adequate powers in obtaining certain personal information. As a result, the reasons given in the document to justify the need for the suggested amendments to the current Acts with respect to production orders for subscriber and service provider are weak and seem to border on infringement of *Charter* rights.

#### Summary

The reasons provided in the document for requiring the drafting and incorporation of the production order into the *Criminal Code* as well as other Acts have not been justified. After examining the mechanisms that are available to law enforcement officials, one can conclude that the reasons provided do not adequately address the need for the creation and incorporation of a production order into our legal system. In light of the fact that law enforcement authorities can use other means to obtain this type of electronic information and, in the event of exigent circumstances, the courts can assist with a court order, it seems unnecessary to give greater consideration to the proposed changes. The recommendations for changes in the document are too extensive and broad. The powers proposed should concern all citizens when we consider and question the extent that the police would be free to determine whether circumstances justify recourse to certain surveillance and, having made such determination, be allowed to use their discretion in defining the scope and duration of the surveillance. No matter how the document is considered, the fact is that this type of electronic access to information would be extremely difficult to regulate and due to the nature of the delivery of the communication, it would be very difficult to identify those situations that would not be justifiable. Members of our society should not be burdened with the worry that their communications via electronic means may be subject to unreasonable search by law enforcement officials. The suggested production orders to obtain



certain information, as currently proposed, would constitute a great violation of privacy rights. The use of electronic devices for communication is considered a private means of communication and, more importantly, is perceived as private communication in many legal relationships. The use of these advanced technologies for the purposes of communications have given rise to the perception that communication through these means are deemed private and not open to examination unless reasonable grounds have arisen. Still, in order to protect our privacy, the courts should be the ultimate judge with respect to the standard of proof required. In considering the proposed orders the focus should be as follows: "the relevant question is not whether criminals must bear the risk of warrantless surveillance, but whether it should be imposed on all members of society."<sup>7</sup>

---

<sup>7</sup> *Massachusetts Supreme Court in Commonwealth v. Thorpe*, (1981) 44 N.E. 2d 250, p. 258



## Data Production Orders

s.19(1)

Implementing a procedural mechanism into Canadian law such as a data preservation order would be a strong statement by the government to ensure Canadians that their law enforcement and national security officials are operating at equal levels with those who commit illegal activities using computer technology and internet access. Modern telecommunications and the use of personal computers to access the internet are, as the Lawful Access Document states, "a great source of economic and social benefits, but they can also be used in the planning, coordinating, financing and perpetration of crimes and threats to public safety and the national security of Canada." Cybercrime is real and it is a threat to everyone in the world, not just to Canadians. The Council of Europe *Convention on Cyber-Crime* calls for the criminalization of certain computer related offences and the adoption of procedural mechanisms to investigate and prosecute cybercrime. The data preservation order is one such mechanism.

The advantages and the central intent of a data preservation order must be clearly relayed to Canadians in order to assure each citizen that such action is necessary in order to distinguish the constantly changing face of crime. Lawful access is a well-established and necessary technique used for investigation. Legal authority is provided in several parliamentary acts and is consistent with the rights and freedoms guaranteed in the *Charter of Rights and Freedoms*. The Lawful Access Document, indicates that most of the required offences already exist in Canada. However, provisions for production orders, data preservation orders and offences relating to computer viruses, must be included in the *Criminal Code* before Canada can ratify the *Convention* and give it effect.

So long as the new proposed orders remain within the rights guaranteed in the *Charter*, such amendments can be seen as being within the natural course of updating our law to reflect new levels of technology that we are experiencing as a nation and a global society.



Many Canadians enjoy the conveniences and benefits of using Internet and wireless communications for business and for personal use. When faced with the possibility of becoming a victim to cyber criminals, it would be reassuring to know that Canada's law enforcement officials are able to protect Canadian citizens from cybercrime and ensure that Internet transactions can be safely completed. The data preservation order is intended, as discussed in the Lawful Access Document and Articles 16 and 17 of the *Convention on Cyber-Crime*, as a tool for law enforcement officials to investigate and prosecute cybercrime. The Lawful Access Document calls for updating the way Canadians protect themselves against new offenders. Data preservation allows law enforcement officials to obtain the necessary evidence required to prosecute those who use the Internet to victimize Canada's citizens and conduct illegal activity more efficiently and discretely than they could before.

Indeed, the question seems to be: Why encourage an offender to conduct illegal activity by using the Internet? The Internet presently offers the cyber-criminal more efficiency and a sense of security – a fingerprintless trail – that no evidence will be left behind. Is it reasonable that a Canadian citizen would accept or support a legal system that allows the offender to take full advantage of Internet and computer technology, while its law enforcement officials are prohibited from doing so? It would appear that being a victim to cybercrime is more violating than the knowledge that the Internet activity of a suspected offender may be stored for investigative purposes.

The concern, however, that data production orders can be seen as an invasion of one's right to privacy is understandable. Therefore, it is crucial that the public is assured that these new updates in lawful access fall within the same realm of acceptable conduct that is now practiced by law enforcement and national security officers. It is important to stress that this is a judicially obtained order and criteria must be appropriately met. The guidelines and limits of the data preservation order must be clearly understood and maintained.

Having agreed that implementing data preservation orders into Canadian law is necessary for updating current security practices and challenging the abilities of the cyber-offender, many issues surrounding implementation must be addressed. Articles 16 and 17 of the Council of



Europe *Convention on Cyber-Crime* discuss guidelines for implementing data preservation orders governing both stored computer data and traffic data. Briefly stated, a preservation order would:

- enable a "competent authority" to order/obtain preserved data stored by a computer system in situations where there are grounds to believe the computer data is particularly vulnerable to loss or modification
- call for the preservation of data for a maximum of 90 days, after which there can be a request for a renewal
- require that the custodian of the data keep all information collected confidential with respect to traffic data
- ensure that preservation would be available whether or not a particular internet service provider was involved in the transmission
- ensure expeditious disclosure to "competent authorities" of sufficient data as to enable to identify the service providers and paths through which the communication was transmitted

Several of the issues brought forth by the Lawful Access Document are considered in the provisions of the *Convention*. Issues relating to legal standards, penalty for non-compliance and how law enforcement officials could impose an exigent preservation order on ISPs must be discussed and guidelines established. The operating details must reflect current lawful access policy and respect *Charter* provisions. The *Criminal Code* of Canada, the *Canadian Security Intelligence Service Act*, and the *Competition Act* provide guidelines for interception and for search and seizure of information. The issuance of data preservation orders, when within the limits of the above statutory law, can be viewed as a natural update to existing parliamentary provisions. Legislative proposals dealing with lawful access must reflect the need to bring the law into accordance with the current state of telecommunication and Internet technology. According to the Lawful Access Document, most of the required offences and procedures provided in the *Convention*, do already exist in Canadian law. Although the data preservation order intends to protect Canadian Internet users and deter cybercrime, there does exist the problem of the practical application of these new orders.



Specifically, there is the reality that Internet service providers and other telecommunication service providers must ensure that the technical capabilities exist in their facilities, which would enable the lawful access by law enforcement and national security agencies. There are real concerns that passing costs to Internet service providers, many of which are small business operations, would be unfair and could potentially cause severe economic consequences. The required system upgrades for Internet service providers have not been discussed by the Lawful Access Document and the cost associated with such upgrades are yet to be addressed. In implementing new legislation based on the provisions of the Council of Europe *Convention on Cyber-Crime*, it is vital that the Government of Canada support the nation's existing Internet service providers. The end result of updating legislation is in the interest of all Canadians. Because a national effort is required to comply with the recommended provisions, it is not unreasonable to assume that the government will have to be accommodating for Internet services providers who already do have the sufficient monitory technology in place, while supportive of the transition for those service providers that do not have this service. Implementing and operating data preservation orders will be dependant on reliable industry response. To ensure a system that works efficiently and is respectful of industry, it is necessary that a procedure regarding confidentiality and legal issues be firmly established, and that implementation and operational costs for service providers responding to data preservation requests are considered.



## The Legal Status of Email

s.19(1)

The use of e-mail as evidence is an issue that is becoming increasingly relevant as society is becoming evermore reliant on computers. Technology has been hurdling forward in leaps and bounds. The law needs to keep abreast with this pace; the law needs to contemplate technology and its many possible permutations to provide greater certainty for both law enforcement and the public at large.

Technology has had such a profound influence on communications that it has changed the way that many people conduct their daily affairs. For example, online bill payments and online banking have experienced a significant increase in users over the last 5 years. So much is done online now that the term "paper trail" should be updated to reflect the realities of the new millennium. Possibly "data trail" will replace this soon to be antiquated term. With this in mind it is certain that law-enforcement will seek computer evidence when building a case against an accused. E-mail is a form of evidence that law enforcement will increasingly rely upon in the future.

The following discussion will demonstrate that e-mail is protected, although not specifically contemplated, by Section 184 of the *Criminal Code*, and Section 8 of the *Charter of Rights and Freedoms*.

Section 184(1) of the *Criminal Code* makes it illegal to intercept private communications in providing:

"Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years".

Section 183 defines private communication as:

"any oral communication, or any telecommunication, that is made by an originator in Canada or is intended by the originator to be received by a



person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.”

The term intercept is explained to include:

“listen to, record or acquire a communication or acquire the substance, meaning or purport thereof.”

E-mail comes within the ambit of Section 183, as it is a telecommunication. Section 35 of the *Interpretation Act* R.S., c I-23 s.1. defines telecommunications in such a broad way that it must include any form of communication that is reliant upon data-transfer technology:

“‘telecommunications’ means the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system”

Telecommunications generally function on the basis of electronic transmissions of impulses. Essentially, the verbal equivalent is broken down into a physical form that can be transmitted by telecommunications technology. E-mail functions in an analogous way. When a computer sends e-mail it is transmitting data-packets that represent the keystrokes of a user, which in turn is a physical representation of that users thoughts.

With the above established, the question that is central to this analysis is whether one has a reasonable expectation of privacy when composing and sending e-mail.

In *R. v. Weir* the defendant was charged with possession of child pornography.<sup>1</sup> During the course of repairing Weir’s e-mail account, his ISP found what they believed to be e-mail messages with child pornography attachments. The ISP immediately informed the police and at the police’s request forwarded the e-mail messages and attachment to them. The police obtained a search warrant, searched Weir’s residence, and seized a computer and disks. The information subsequently extracted from the computer was found to consist of the original e-mail message

<sup>1</sup> *R. v. Weir*, [1998] A.J. No. 155.





and attachments, and other stored data that was construed as child pornography. At trial, Weir challenged the legality of the actions of his ISP and the police. He argued that the ISP breached his right to privacy to his e-mail. Weir also characterized the asking for and receipt of the e-mail message by the police as a warrant-less search and seizure.

Justice Smith explains that e-mail saved at an ISP carries a reasonable expectation of privacy. Therefore, judicial pre-authorization (a warrant) will usually be required to search and seize it. He then goes on to discuss the nature of e-mail versus the nature of letter mail in paragraphs 72 to 77 of his judgment. When sending letter mail there is a different expectation of privacy between the contents of the envelope and the cover of the envelope. The cover is exposed to anyone who is handling the mail, thus the information on the cover carries a lower expectation of privacy than does the contents inside.

E-mail has an analogous format to letter mail. E-mail is directed by a header to its intended destination. A header is an e-mail's "footprints in the sand", it can be used to trace an e-mail's history from its origin to destination.<sup>2</sup> Repair work to e-mail can be done through headers. The headers are like the information printed on the outside of the envelope; their semi-public nature imports a lower expectation of privacy.

Smith J goes on to discuss the difference between the concept of "cover" in relation to regular mail and e-mail:

...in first class mail the cover is respected. In e-mail, the cover is (or was in June of 1996) routinely violated in order to repair the technology. There are two or three levels of violation depending on the type of repair done and excluding a repair done by deleting the message or by enlarging the e-mail box. The size of the attachments may be viewed. The list of attachment names may be viewed. The message itself may be opened which can include looking at the message and the attachments or either. These facts about the technology help me to conclude the e-mail message is unlike first class mail in the level of privacy that it can attract.

Another difference between e-mail and first class mail is that in order to make an e-mail message truly private, one can encrypt it. The evidence (of Mr. Boeske) is that encryption, although readily available, is not yet widely used by the general

<sup>2</sup> For further discussion on headers see <http://support.xo.com/abuse/guide/guide2-mail2.html>.



public. However, the debate in the United States over whether there should be publicly regulated bodies for deposit of encryption keys to permit reading of encrypted e-mail, suggests that encrypted mail is, for all practical purposes, unreadable and, therefore, privacy is secured. That encryption is relied on by some e-mail users to ensure privacy, and that it is not yet used widely by the general public underscores the need for legal protections.

In summary, I am satisfied e-mail via the Internet ought to carry a reasonable expectation of privacy. Because of the manner in which the technology is managed and repaired that degree of privacy is less than that of first class mail. Yet the vulnerability of e-mail requires legal procedures that will minimize invasion. I am satisfied that the current Criminal Code and Charter of Rights protections are adequate when applied in the e-mail environment."

Although Smith J concludes that the expectation of privacy accorded to e-mail is lower than that of letter-mail, he also recognizes that this is due to the nature of current technology. E-mail is vulnerable to disclosure while an ISP is repairing an account. Headers are not usually encrypted which leaves exposed information regarding the addresses to which the message is destined, and from which it came. However, this implies that as technology advances and encryption methods advance, the expectation of privacy in e-mail will likewise increase.

Another notable point is that letter-mail is generally exposed to individuals employed by the postal service. The handling of mail is governed by the *Canada Post Corporation Act* 1980-81-82-83, c.54,s.1. Sections 48, 49, and 50 make it an offence for anybody without authorization to "knowingly open, keep, secrete, delay, detain, or permit to be opened" or "knowingly abandon, misdirect, obstruct, delay or detain" mail or the method of mail delivery. Similarly there should be guidelines imposed on ISP's and any other body that deals with any aspect of the transmission of e-mail.

*R. v. Plant* is further support for the proposition that e-mail requires legal protection as it is a communication with a reasonable expectation of privacy.<sup>3</sup> The accused Plant appealed his conviction of unlawful cultivation of marijuana and possession of marijuana for the purposes of trafficking. The police had received an anonymous tip, which led them to check the electrical utility's computer to assess the electrical consumption at the address obtained from the tipster. It was determined that consumption was four times greater than the comparable average. The

<sup>3</sup> *R. v. Plant*, [1993] 3 S.C.R. 281.



police then obtained a search warrant for the premises. One of the bases of Plant's appeal was whether the police use of computerized electrical records violated Section 8 of the *Charter*. McLachlin J makes the following statement in her judgment:

The question in each case is whether the evidence discloses a reasonable expectation that the information will be kept in confidence and restricted to the purposes for which it is given. Although I find the case of electricity consumption records close to the line, I have concluded that the evidence here discloses a sufficient expectation of privacy to require the police to obtain a warrant before eliciting the information. I conclude that the information was not public, since there is no evidence suggesting that this information was available to the public and the police obtained access only by reason of a special arrangement. The records are capable of telling much about one's personal lifestyle, such as how many people lived in the house and what sort of activities were probably taking place there. The records tell a story about what is happening inside a private dwelling, the most private of places. I think that a reasonable person looking at these facts would conclude that the records should be used only for the purpose for which they were made - the delivery and billing of electricity - and not divulged to strangers without proper legal authorization.

The qualities of electricity consumption records that McLachlin J cites in favor of these records being private are also qualities that make e-mail data private. These qualities are the following: that there is a reasonable expectation that the data will be kept confidential and that the data will be used for the purpose for which it is given; the data is not public; and that the data, or records, reveal information about an individual's personal/private lifestyle. The aforementioned qualities are all inherent in e-mail. E-mail is used for the purpose of relaying messages between individual users. It is generally expected that e-mail will remain confidential, depending on the nature of the information disclosed within the e-mail. Some e-mail is intended to be forwarded between users (depending on "netiquette"). Such e-mail is usually of an impersonal nature and would not likely be the subject of the interest of law enforcement as they are generic and do not reveal any important information about the sender. As well, e-mail often reveals personal information about an individual's lifestyle. The reality of modern life is that society is becoming increasingly dependant upon computers and will continue to develop a greater reliance upon e-mail as a mode of daily communication.

Section 8 of the *Charter* provides that everyone has the right to be secure against unreasonable search or seizure. In *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, Wilson J, at paragraph 86 of his judgment explains that Section 8 applies not only to the protection of an individual's property, but also to their reasonable expectation of privacy.<sup>4</sup> Furthermore, Wilson J quotes *Hunter v. Southam*, where Dickson J states:

The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether it is expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.<sup>5</sup>

Both sections 183 of the *Criminal Code* and Section 8 of the *Charter* make it abundantly clear that an individual's reasonable expectation of privacy must be considered when justifying the infringement of a person's right against unreasonable search and seizure. In *Hunter v. Southam*, Dickson J explains that to validate governmental intrusions upon an individual's expectations of privacy, the governmental actor must obtain prior authorization, where it is feasible, from a person "capable of acting judicially." To obtain such prior authorization the governmental actor must establish, upon oath, reasonable and probable grounds to believe that an offence has been committed and that there is evidence to be found at the place of the search.

E-mail should receive the same treatment by the Canadian Government as regular mail, as it is afforded the same protections as a private communication. Thus the statutory and common law rules of evidence will have equal application to e-mail as they do to regular mail. It is not necessary for Parliament to update the relevant sections of the *Criminal Code* such as the definition of telecommunications found in Section 183. E-mail is by definition included in this section. The definition of telecommunication was probably, as mentioned before, made so broad and expansive to allow for the law to accommodate new technologies. To define

<sup>4</sup> *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 425.

<sup>5</sup> *Hunter v. Southam*, [1984] 2 S.C.R. 145.



Internet Innovation Centre – Internet Law Group

---

telecommunications by reference, the specific forms that it is currently embodied by would not accommodate the need for law to develop concurrently with the rapid pace of technological growth.

What appears to be needed is statutory control of ISP's. Although ISP's are private bodies, the fact that they provide such a crucial service to Canadian citizens is cause for concern.<sup>6</sup> For any body that carries out a service of such extreme importance as mail delivery, state imposed regulations are necessary.

---

<sup>6</sup> See the News.com article at: [http://news.com.com/2100-1023-963631.html?tag=fd\\_lede2\\_hed](http://news.com.com/2100-1023-963631.html?tag=fd_lede2_hed) for further discussion.



## Lawful Access Legislation in the United States and United Kingdom

s.19(1)

The Canadian Parliament is proposing to enact new legislation and to amend current legislation to allow for lawful interception of wireless and Internet communications. Other countries, including the United States and the United Kingdom, already have similar legislation in place. The United States passed the *Communications Assistance for Law enforcement Act* ("CALEA") in 1994. In United Kingdom, *The Regulation of Investigatory Powers Act* received Royal Assent on July 28, 2000. Both of these acts have addressed many of the issues that the Canadian Department of Justice has identified in the Lawful Access Consultation Document and should be considered in the drafting of Canada's lawful access legislation.

An integral part of the legislation/amendments proposed by the Canadian Department of Justice would require all wireless and Internet service providers ("ISPs") to provide technology to enable law enforcement agencies to monitor the activity of their customers, once a warrant has been obtained.<sup>1</sup> In the United States CALEA requires telecommunications carriers to ensure that their equipment, facilities, and services are able to comply with authorized electronic surveillance.<sup>2</sup>

CALEA provides that the Attorney General is to estimate the actual number and maximum capacity of communication interceptions that government agencies may conduct and the number of pen registers, and trap devices that government agencies will use. The Attorney General is to make this estimate after consultation, notice and comment of law enforcement agencies, telecommunication carriers, telecommunication support services and telecommunication

<sup>1</sup> R. Chandarana, "Canada Cyber-Snooping Plan Raise Ire" *Mail Utilities News* (25 September 2002), online: Mail Utilities News <<http://www.mailutilities.com/news/2043.html>> (last modified: 25 September 2002).

<sup>2</sup> "Communications Assistance for Law Enforcement Act (CALEA)", online: Federal Communications Commission <<http://www.fcc.gov/calea/>> (date modified: 4 April 2002).



equipment manufacturers. After notice of this estimate telecommunication carriers are given approximately 4 years to modify their systems to accommodate the estimate.<sup>3</sup> This appears to be a reasonable time period to implement the required changes and the estimate should be reasonable as it is determined after consultation with the telecommunications industry. Telecommunications carriers are provided with a maximum capacity of accommodation that they are not required to exceed, as such they will have general foresight of the extent of burden placed upon them by this legislation.

In accordance with CALEA, telecommunications carriers are to ensure that interception of communications or access to call-identifying information is activated only in accordance with a court order or other lawful authorization with the intervention of an officer/employee of the carrier acting in accordance with regulation.<sup>4</sup> This provides a safeguard to ensure that communications are not intercepted without proper authority and that regulations are being followed in the interception of communications.

In the Lawful Access Consultation Document, the Department of Justice asks whether regulations should provide for fees to be paid to a service provider for operational assistance.<sup>5</sup> CALEA addressed this issue by providing that the Attorney General may agree to pay for all reasonable costs directly associated with the modifications performed by telecommunications carriers performed before January 1, 1995. Upon petition from the telecommunications carrier, the Attorney General may agree to pay for costs incurred by the telecommunications carrier after January 1, 1995.<sup>6</sup> Telecommunications carriers will likely be more willing to comply with the required modifications when the modifications are paid for by the government than if the telecommunications carrier is to bear the costs of modifications.

<sup>3</sup> Communications Assistance for Law Enforcement Act of 1994, s.104 (1994), online: Communications Assistance for Law Enforcement Act <<http://www.askcales.ca/>> (date accessed: 25 October 2002). [hereinafter "C.A.L.E.A."]

<sup>4</sup> C.A.L.E.A., *supra* s.105 (1994).

<sup>5</sup> Department of Justice Canada, "Lawful Access-Consultation Document"(2002), online: Lawful Access Consultation Document <[http://canada.justice.gc.ca/en/cons/la\\_al/](http://canada.justice.gc.ca/en/cons/la_al/)> (last modified: 26 August 2002). [hereinafter "Department of Justice"]

<sup>6</sup> C.A.L.E.A., *supra* note s.109



Compliance is addressed as an issue to be considered in the Lawful Access Consultation Document.<sup>7</sup> Non-compliance with the requirements of CALEA may result in the imposition of a civil penalty of up to \$10,000 per day for each day in violation of a court order.<sup>8</sup> This penalty appears to be harsh, but it is the maximum penalty and is only a civil sanction to which no criminal liability is attached.

Once wireless and Internet service providers are capable of providing the technology to enable law enforcement agencies to monitor the activity of their customers, regulations guiding interception must be enacted. *The Regulation of Investigatory Powers Act* describes the requirements for lawful interception of communication in the course of its transmission by means of a public postal service or a public telecommunication system.<sup>9</sup>

The Canadian Department of Justice asks under what conditions customer information should be made available.<sup>10</sup> In addressing this issue, *The Regulation of Investigatory Powers Act* requires that unless the sender or recipient of the communication has consented to the interception, an interception warrant must be obtained.<sup>11</sup> An interception warrant will be issued only if the Secretary of State believes the warrant is necessary for purposes of national security, preventing or detecting serious crime, or giving effect to provisions of any international mutual agreement in order to prevent/detect serious crime. It must also be established that the conduct authorized by the warrant is proportional to what is sought to be achieved by that conduct and that the information cannot be obtained by other means.<sup>12</sup> The requirement of a warrant, the circumstances required to obtain a warrant and the condition that no other means of obtaining the information exist, ensure that the interception of communication is limited to particular circumstances. The use of a proportionality test balances the interception of communication with human rights.

<sup>7</sup> Department of Justice Canada, *supra*

<sup>8</sup> C.A.L.E.A., *supra* note s.201

<sup>9</sup> "Explanatory Notes to Regulation of Investigatory Powers Act", online: Explanatory Notes to Regulation of Investigatory Powers Act <<http://www.hmsso.gov.uk/acts/en/2000en23.htm>> (date accessed: 25 October 2002).

<sup>10</sup> Department of Justice Canada, *supra*.

<sup>11</sup> Regulation of Investigatory Powers Act 2000 (U.K.), 2000, c. 1, s. 3, online: Regulation of Investigatory Powers Act 2000 <<http://www.hmsso.gov.uk/acts/acts2000/20000023.htm>> (date accessed: 25 October 2002). [hereinafter "Regulation of Investigatory Powers Act"]

<sup>12</sup> Regulation of Investigatory Powers Act, *supra* note c. 1, s. 5.





Unless the interception warrant confines the authorized conduct to the interception of external communications in the course of their transmission, or a certificate is attached certifying the description of intercepted material which is necessary for national security, preventing or detecting serious crime, or the economic well-being of the United Kingdom, *The Regulation of Investigatory Powers Act* requires that an interception warrant name or describe one person as the intercept subject or a single set of premises in which the warrant is to take place. Warrants describing communications to be intercepted must set out factors such as addresses, numbers, apparatus etc. that are to be used for identifying communications which are likely to be/include communications from or intended for the person or premise named or described in the warrant.<sup>13</sup> These requirements ensure that interception only occurs in specific situations in regard to specific information, putting a reasonable limit on the scope of interception.

*The Regulation of Investigatory Powers Act* requires that a person who has been served a copy of the interception warrant for purposes of assistance is under a duty to take all reasonably practicable steps for giving effect to the warrant as notified to him by the person to whom the warrant is addressed. *The Regulation of Investigatory Powers Act* deals with the issue of compliance mechanisms by imposing criminal liability upon a person who knowingly fails to comply with their duty. The maximum punishment on conviction is a term of imprisonment for a term not exceeding two years, or a fine, or both. The duty to take steps for giving effect to a warrant is also enforceable by civil proceedings by the Secretary of State for an injunction or for specific performance.<sup>14</sup> The imposition of a criminal conviction is a harsh punishment for non-compliance, but the person under a duty is only required to take steps which are reasonably practicable, as such the burden of compliance is reasonable.

*The Regulation of Investigatory Powers Act* includes provisions ensuring that a person who provides a postal service or telecommunications service will receive a fair contribution towards the costs incurred in relation to carrying out interception warrants. The Secretary of State may provide for payments to be made out of money provided by Parliament.<sup>15</sup> As discussed earlier,

<sup>13</sup> Regulation of Investigatory Powers Act, *supra* note c. 1, s. 8.

<sup>14</sup> Regulation of Investigatory Powers Act, *supra* note c. 1, s. 11.

<sup>15</sup> Regulation of Investigatory Powers Act, *supra* note c. 1, s. 14.



the contribution of costs by Parliament is likely to make the telecommunication provider more willing to comply with the regulations and carry out the interception warrant.

The Canadian Department of Justice asks what kind of procedural safeguards should be included for production orders.<sup>16</sup> *The Regulation of Investigatory Powers Act* includes various safeguards. Regarding the intercepted material, the number of persons to whom the material is disclosed, the extent to which the material is disclosed, the extent to which the material is copied and the number of copies that are made must be limited to the minimum that is necessary for the authorized purpose. Each copy of the material that is made must be destroyed as soon as there are no longer grounds for retaining it as necessary for the authorized purpose.<sup>17</sup> These safeguards minimize the interception and disclosure of communication to what is necessary to carry out the purposes set out in the warrant. The Act has also set out provisions for a Technical Advisory Board. A person who has been issued a notice to provide assistance may refer the notice to the Technical Advisory Board which has the authority to either withdraw the notice or give further notice confirming the effect of the initial notice with or without modifications.<sup>18</sup> This procedure is a safeguard of the legitimacy of interception.

In enacting lawful access legislation it is necessary to balance human rights with the need for effective interception measures. The United States and the United Kingdom legislation discussed have given law enforcement agencies the authority to intercept communications and have balanced this authority with procedures and safeguards to protect the public and telecommunications providers from unreasonable interception. Many aspects of the legislation discussed could reasonably be employed in the proposed Canadian legislation.

*The Communications Assistance for Law Enforcement Act* currently in place in the United States is of assistance to Canadian Parliament in drafting legislation requiring wireless and Internet service providers to provide technology to enable law enforcement agencies to monitor the activity of their customers once a warrant has been obtained. Provisions of this Act that Canadian Parliament may want to implement include the consultation process with

<sup>16</sup> Department of Justice Canada, *supra*.

<sup>17</sup> Regulation of Investigatory Powers Act, *supra* note c. 1, s. 15.

<sup>18</sup> Regulation of Investigatory Powers Act, *supra* note c. 1, s. 12.



telecommunication industry representatives in setting the maximum capacity of accommodation, the payment of fees to telecommunications carriers for costs incurred in meeting the requirements of the legislation, and the imposition of monetary fines for non-compliance.

*The Regulation of Investigatory Powers Act* in place in the United Kingdom provides guidance to the Canadian Parliament in enacting legislation regulating the interception of communications. Provisions of this act which may be beneficial to Canadian legislation include the requirement of specific information to be described in an interception warrant, the imposition of a duty to take only reasonable and practicable steps in giving effect to a warrant, the contribution of costs to the telecommunication carrier, the implementation of a Technical Advisory Board and the other safeguards employed. The imposition of criminal sanctions for non-compliance may be too harsh, but civil proceedings are reasonable.



## The Lawful Access Consultation Document and The American Carnivore System

s.19(1)

The Carnivore system is much less intrusive than the blanket surveillance system that the Lawful Access Consultation Document ("LACD") proposes.<sup>1</sup> As a first step a warrant is required to initiate surveillance. At this point the FBI brings in a computer which is attached to the host ISP. This computer runs a packet sniffer program which sniffs out data packets from the suspect computer's IP address. It can also be set to intercept only data packets related to any set of criteria. The packets are then run through a program which reconstructs them into their original, useful, format. These data packets can include everything that the computer does, from sites visited to transmissions sent and received and even files being utilized by the suspect computer. This information is then stored on a removable zip drive for later pickup by the FBI. The zip drives are picked up and placed into sealed containers. This system has the potential for abuse but it is much less intrusive than the shift from targeted to universal surveillance that the LACD includes. The LACD proposes storing all activities of all Internet users in Canada. The LACD will in effect turn Internet service providers and telephone companies who retain email and Internet records into an arm of the police.

The American warrants for using the Carnivore machine are re-evaluated on an ongoing basis to ascertain whether there are grounds for continuing the surveillance of the Internet.

### Problems

Even if we were to adopt a less intrusive Carnivore style system of Internet surveillance, Canadian law may require separate warrants for different computer functions. E-mail, sites

<sup>1</sup> For a summary on how the Carnivore system operates, see <http://www.howstuffworks.com/carnivore.htm>.

visited, and files used could perhaps not all be covered by the same warrant due to the differing levels of privacy expected for each of these activities.

There are a number of problems with the LACD plan as it stands. Encryption would likely defeat any Internet surveillance program or system. Those with something to hide would likely encrypt their files and communications thus rendering them indecipherable to the police or even the FBI. The sniffer programs would fail to pick up on the content of the file and thus let it go. Even if the sniffer were set to intercept all encrypted messages these would be useless as the encryption likely could not be broken. Furthermore, anyone who was going to hide their communication would likely send it from a public computer thus making it almost impossible to intercept or find. This would render the entire system useless. Foreign languages would again likely defeat a sniffer program looking for pertinent materials unless it were set to that particular language.

A more pressing legal issue is that of the retention of all of the user data. With the Carnivore system the data relating to a suspect computer is stored on a zip drive which is then sealed in a container so that no one can tamper with it. If the LACD plan were to go through the realms of information kept at the ISP, presumably the data would not be subject to such close security and tampering would be an issue. This would likely render any such information inadmissible at court thus rendering the entire program moot. It could also lead to some very misguided investigations based on altered or misleading information. ISP employees would likely have access to these files thus bringing up the issue of invasion of privacy relating to their ability to snoop in peoples' files.

The fact remains that any such surveillance program could not establish who it was exactly that used the computer to perform the recorded activities. The user is not necessarily the subscriber at the ISP. This leads to other legal problems such as surveillance of people without reasonable grounds and wrongful prosecutions.

If any such surveillance system is going to be implemented the laws of Canada will likely have to be revised to make this sort of program possible and legal. As the law exists right now a

universal surveillance system would likely be struck down as an invasion of privacy and abuse of power.

Similar proposals have been initiated in the EU have been met by public outcry and outright refusal by ISPs. "What would the citizens of Europe and elsewhere do if they were told a law had been passed allowing what they sent through the post to be routinely read by the police at any time?" Mr. Lock Coriou (Reporters Sans Frontieres) asked in a *Guardian Unlimited* interview. "They would be outraged at such restrictions on their freedom. Yet these are exactly the kind of measures that have been or are being taken concerning the Internet. We need to be much more vigilant," he warned. Canadian phone companies do not store phone records or record all telephone conversations. Snail mail is not tracked or photocopied or read by Canada Post. Why should Internet communications be any different? Why should they be recorded in their entirety without a warrant, without reason, at the communication provider's expense, and all this for later perusal at the leisure of the police? The Lawful Access Consultation Document suggests that all communications providers may have to start doing exactly that.

### Recommendations:

The LACD recommendations as they currently stand are completely airy fairy. They have no real substance and no real plan of how to actually implement the program. This shows a dangerous disregard for the possibility of offending Canadian law and complete ignorance of the technical feasibility of the plan. The logistics of storing everything that everyone in Canada does on the Internet is bewildering. The volume of data to be stored is huge. Even if it were only to be stored for a few months at a time it would be so massive as to render the storage impossible and astronomically expensive to even attempt. Adopting an American Carnivore style system would solve these problems and would also reduce the invasion of privacy and thus the likelihood of offending Canadian law. It would cause less interference with ISPs and less shifting of state and police responsibility onto unwilling ISPs.

This system may allow for preservation orders as a stopgap measure if absolutely necessary. The police could request an ISP to retain a single suspect's transmissions while in the process of

Internet Innovation Centre – Internet Law Group

---

obtaining a warrant. Then when the warrant has been issued the transmissions could be released to the police. If no warrant is obtained then the recorded transmissions should be destroyed.



## **The Dream of Safety: Should Canada Ratify *The Convention on Cyber-Crime*?**

s.19(1)

If Canada is to adopt and ratify *The European Convention on Cyber-Crime*, amendments to the *Criminal Code* and other statutes will need to be drafted to facilitate search and seizure of electronic information (be it from the Internet or from wireline/wireless communications). Current proposals from the Minister of Justice include: an onus on service providers to have data preservation and production capability, a low expectation of privacy for customer information and traffic data, four-day data production orders served by law enforcers without judicial notice, and possible seizure of e-mail.<sup>1</sup> This paper will consider whether the proposed legislation is justified in a broad ethical sense, and, more narrowly, whether the specific methods of information seizure are justifiable.

The first matter that needs to be reviewed is the 'mischief' at which the legislation is aimed. Are we experiencing an epidemic of cyber-crime? Is it the same thing as "cyber-terrorism"? The former connotes a rather sordid group of long-standing offenses such as possession of child pornography, fraud, drug trafficking, and price-fixing. Cyber-terrorism, on the other hand, is more a product of its time. Specifically, post 9/11 and the American "War on Terror" and mostly connotes threats of national and/or corporate security, though it may include computer virus production. It would be a considerable stretch of reason to say that there is an epidemic of cyber-terrorism, but the proposals could be ratified on the pretext of an avoidance of a potential emergency situation. Whether the proposals are justified or not is a matter of balancing the need for the legislation versus the potential infringement on privacy and/or individual rights.

The proposals assume that law enforcement agencies are currently at a disadvantage. Although practically anything a person does on, say, the Internet may be tracked, there are no *Criminal*

<sup>1</sup> See [http://canada.justice.gc.ca/en/cons/la\\_al/d.html](http://canada.justice.gc.ca/en/cons/la_al/d.html).





*Code* provisions that specifically allow for the search and seizure of this electronic information. Since the Internet may be accessed from any machine hooked up to a service provider, a 'cyber-criminal' might use a public-access computer (e.g. a community access site) to perpetrate cyber-crimes, hence leaving their personal home computer (if he/she owns one) free of illegal materials should it be seized and searched. In reality, the actual probability of this is somewhat slim. In the case of child pornography, it is far more likely that a person will download such materials in the privacy of their own home, away from prying eyes. However, there is nothing in the proposed legislation that would effectively enable police to monitor public access sites and prevent, for example, drug transactions done under pseudonyms. The crimes that may be traced at all are therefore more likely to be traced to a personal home computer, and the procedures for seizure in that case do not require any new enabling legislation.

In an attempt to justify the proposals, the Lawful Access Consultation Document refers to The Solicitor General's Annual Report on the Use of Electronic Surveillance, which claims that the conviction rate for cases where lawful interception evidence is used or adduced in court is greater than 90%. Effectiveness, however, should not be the sole justification of legislation. Allowing the possibility that the interception is effective in convicting people, the numbers alone do not indicate whether all 90% were actually guilty of committing crimes. It may be that the legislation is *too* effective, and would lead to a rash of undeserved convictions. In an era when civil liberties are in grave danger of being subordinated to the dream of national safety, every incremental step away from civil liberty brings the Orwellian nightmare closer.

What is the potential infringement on privacy and/or individual rights? One proposal would allow a four day preservation of data order without judicial order where obtaining that order is "impracticable". The data referred to in this proposal has a lower expectation of privacy than private communications: subscriber identity information and probably traffic information (i.e. who the person called, which sites were visited, what was downloaded). E-mail does not apply because of the higher expectation of privacy. Still, the ability of law enforcement agencies to order either the production or preservation of four days worth of traffic data without judicial order could easily lead to abuse of power and injustice. Persons may be targeted on the basis of race alone (and with 'cyber-terrorism' this is more than a remote possibility). Moreover, the



information that is thus obtained is of questionable worth, considering the ease with which it may be misinterpreted. For example, suppose a 21 year old male is an avid lover of pornography, and has a special interest in 18 and 19 year old girls. He may be disgusted by child pornography, but the keywords he enters and the sites he might accidentally visit could be construed as compelling evidence of a very serious nature, despite the fact that he is not a criminal! Similar misconstructions could be made in the cases of people interested in political activism that wander onto terrorist sites, or Islamic people unaware that a person or organization is affiliated with terrorism.

The proposals argue that there is a low expectation of privacy regarding this material, drawing an analogy with existing legislation that allows for the compilation of a list of phone numbers that a suspect phoned during a certain period of time. The reasoning stems back to *R. v. Plant*, in which the Supreme Court of Canada held that a person could not reasonably expect privacy regarding personal information that does not reveal intimate details of personal and/or lifestyle choices.<sup>2</sup> A paradox emerges: if the information does not reveal anything personal or intimate, then its use to law enforcement officials is questionable. Conversely, if the information is useful, it must be fairly revealing and people may reasonably expect some privacy; thus, the police should not be able to obtain it without judicial order.

The proposal states that it does not demand general data retention--that is, keeping every user's traffic information regardless of suspicion--but there is a lack of clarity on the issue. Civil libertarians have been vocal in their claim that the proposed legislation violates the presumption of innocence (whether it be in the Canadian *Charter of Rights and Freedoms* or the *International Bill of Rights*). Although it seems that service providers are not required to store traffic information without some kind of official statement of suspicion from a law enforcement agency, the proposal never explicitly states this in clear terms. Furthermore, the retroactivity of a production order is neither affirmed nor denied, so it is uncertain if police could request that a user's traffic information from the previous two weeks be produced.

---

<sup>2</sup> *R. v. Plant*, [1993] 3 S.C.R. 281.



The language of the proposal is clearer regarding e-mail. Police do not have the power to intercept or seize e-mail correspondence without judicial orders. This stems from a higher expectation of privacy, but the level of expectation is unclear. The proposals are unsure whether an e-mail is a private communication, and as such whether it should be subject to the same stringent standards of procedure as the interception of a letter requires. The alternative analogy is with a recorded message sent on tape in the mail, which courts have found does not have the same expectation of privacy, as it is foreseeable that someone else will hear it.<sup>3</sup> It is clear that if a letter may be lawfully intercepted, there should be the capability of intercepting e-mail as well, but under which standard?

I argue that the same procedure that precedes the interception of a posted letter should be applied to e-mail. E-mailing requires a password, a clear indicator that there is a reasonable expectation of privacy. Secondly, the form of communication is the same as a letter (unless, of course, the e-mail is c.c.'d to numerous recipients); a person transcribes the thoughts they wish to communicate, then they may edit them and ultimately send them to a specified receiver. Thirdly, the language of e-mail is typically informal. People are not generally on guard against implicating themselves, nor do they always take pains to be clear (unlike letters, you can always e-mail a quick correction). E-mail language is also subject to more rapid evolution than ordinary correspondence, quickly becoming an *ad hoc* collection of new terms or new meanings applied to old terms. Thus, there is a real danger of unintended meaning, as correspondence is read out of the context of its "thread". The net result is that any lowering of the procedural standard for interception would create unjustifiable legislation.

The specific method of information seizure is itself unjustifiable, in that it places the onus entirely on service providers to have and implement the technology necessary to produce traffic information and to intercept communications. While it is true that the large, corporate service providers such as Roger's Communication may already have the technology to do so, smaller companies may not have the technology, and it would be imposing an unfair burden on them to require it. The proposal requires the cost to be borne by the service providers when a "significant upgrade" is required; the cost of minor changes will be borne by the government. In

<sup>3</sup> The permanence of tapes is used as a justification, as though it were somehow easier to erase a letter!



practice, this means that large companies or corporations will receive funding to upgrade, while smaller providers are effectively shut down.

The proposed legislation thus completely absolves manufacturers of any responsibility regarding the enabling of tracking or information seizure. Some hardware such as cell phones or modems are more traceable than others; cell phones may have a distinctive frequency, and modems may send serial number information to every site it connects to or downloads from. Since many people, law-abiding or not, have an aversion to the idea that someone may be watching them at any time, manufacturers are thus encouraged to develop hardware that is less traceable. A vicious circle develops, analogous to the late 20<sup>th</sup> century blossoming of radar detectors and 'radar detector detectors'. Service providers would need to constantly scramble to keep up with the latest firewalls, etc., because of the public's desire to feel unobserved<sup>4</sup>. Thus, it would be fairer to prohibit the manufacture of "untraceable" cell phones or modems, instead of placing the entire onus on service providers.

What conclusions can be drawn from the foregoing discussion? Cyber-crime, whether or not the problem is real, impending, or imagined, is being used as a justification for proposed legislation that is in grave danger of curtailing rights of individuals to privacy. The most serious potential breaches of civil liberties stem from the following proposals:

1. that law enforcement officials be able to obtain traffic information without judicial notice;
2. that there is no clear language prohibiting retroactivity of production orders;
3. that single-recipient e-mail be treated as somehow 'less private' than a mailed letter; and
4. that service providers carry the burden of upgrading, without reference to manufacturers.

If these four potential problems are avoided, the proposed legislation will be significantly more justifiable.

---

<sup>4</sup> This feeling may be illusory, since most movements are tracked by large service providers who already track movement on their server (and small providers are themselves subscribers to larger providers and are thus only one step removed).



**Pierlot, Paul**

---

**From:** Dean RAVELLI [Dean.Ravelli@rcmp-grc.gc.ca]  
**Sent:** 2002 Dec 13 3:45 PM  
**To:** la-al@justice.gc.ca  
**Cc:** Brian MCLEOD  
**Subject:** LAWFUL ACCESS AMENDING LEGISLATION

Pls be advised that we have reviewed the proposed changes to the legislation and on behalf of Insp B.K. McLEOD OIC Strathcona County Detachment we support the proposed amendments.

D. Ravelli, Sgt for Insp B.K. Mcleod.

**Pierlot, Paul**

s.19(1)

**From:** [REDACTED]  
**Sent:** 2002 Dec 13 3:56 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Lawful Access Consultation Input

Hello

Please accept my email as a reply to your call for input on the Lawful Access consultation document.

In general, I am opposed to the proposals. I believe they unduly prejudice the online activities of the individual. I think they will put an undue onus on ISPs and other online service providers. I am concerned that the privacy and security of the online individual is at much greater risk from other online criminal activity such as identify theft and database break-ins, and inappropriate service provider conduct, than any other source. These proposals do nothing to address those issues.

I would like the following specific points to be carefully considered in any development of new online privacy, security and lawful access legislation or regulation:

#### NO JUSTIFICATION

1) It is not clear to me that changes considered under the proposals would contribute in any meaningful way to combating crime or terrorism. No solid case has been made to establish the benefit of access to an individual's online activity in such a context. No evidence has been tabled to demonstrate that Canadian ISPs were a witting or unwitting participant in any terrorist activity. No evidence has been tabled to show that the recording of online activities will be useful in anyway when attempting to prevent crime or terrorist activity.

#### CONTROL COSTS

2) Should they proceed, the costs of any new access activities taken under proposed laws should not be passed onto the ISP, or the end client, for that matter. Any undue financial onus on Internet service providers or users would have negative effects on service, support and subscriber levels, I believe. The appropriate government agency, be it the Justice Department or a Crown attorney, should pay for all such activities, and all associated costs should be clearly declared and available to the public.

#### CONTROL ACCESS

3) Should the activity and content of any individual's online activity be subject to lawful access as proposed, I believe that changes to the Criminal Code should be considered, in order to clarify, restrict and otherwise control access to such records. A formal search warrant, sworn by a recognized law enforcement official, and approved by a sitting judge or other identifiable judicial official, must be made. All access documentation should accompany the case documentation and/or court docket, if one results, and be available without fee to the public.

#### PENALIZE UNLAWFUL ACCESS

4) As well, severe penalties must be in place before the collection of online activity records begins, in order to punish anyone obtaining, or attempting to attain, online activity records without due process and

legal authorization. The existence of such a database as considered under these proposals creates a very attractive target for online hackers, criminals and the like.

A mechanism to identify if necessary any and all ISP employees, full- or part-time, or any consultant or contractor of the ISP, should be in place to help protect access to the valuable records being collected.

#### 5) INDIVIDUAL ACCESS

I believe that, as a protection for online users, the individual should always be allowed access to his or her online repository of activity, without charge, penalty or prior permission. The right to address inconsistencies, inaccuracies or misrepresentations in such records should be a built-in right of individual access, and a tribunal should be in place to hear and adjudicate conflicts, should they arise.

#### 6) EVALUATION AND ASSESSMENT

Should any new laws or regulations be put into place regarding Lawful Access to online activity, such laws or regulations should come up for careful public scrutiny and evaluation in a pre-determined timeframe; I suggest within the first year, and at each subsequent annual anniversary as long as such laws are in place. A further call for public input and consultation should accompany each review process.

Thank you for the opportunity to have input on this process; I look forward to the time when results of the consultation process are made public.

Toronto, ON

s.19(1)

Pierlot, Paul

---

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 15 11:29 PM  
To: la-al@justice.gc.ca  
Subject: Submission on "lawful access"



Untitled

Attached, in HTML format, is my submission to the "lawful access" comment process.



Embrace and defend.



# Protecting lawful private communications: Submission of [REDACTED]

s.19(1)

## Introduction

Canadian society is founded on core values of respect for human rights, including the rights to privacy; assembly and association; free expression; and personal property. Criminal and terrorist activity threatens those basic rights, and accordingly, Canadian institutions protect our rights by opposing criminal and terrorist activity. It is crucial that institutions must not accidentally destroy the very rights they are trying to defend. In this submission to the "lawful access" public consultation process, I argue that current proposals to change Canadian law in the name of fighting terrorist and criminal activity, would in fact endanger our rights without achieving the stated goal of defending Canadian interests.

The consultation process is flawed because it assumes its own conclusion. It is further flawed by unsupported and incorrect technical assumptions about the Internet and how an "access" scheme would or could work. The proposal is riddled with implementation problems. It would destroy non-profit Internet Service Providers (ISPs) and shift authority for searches from the police (where the authority belongs) to ISP staff. Finally, the proposed prohibition on mere possession of destructive "devices", an issue only vaguely related to "access" at all, raises the same problems for freedom of thought as the infamous U.S. Digital Millennium Copyright Act; it must be rejected out of hand.

## This process assumes its own conclusion

The phrasing of the "consultation" document is a great disappointment because it is apparent that although the

document claims to be asking questions, it is in fact assuming specific answers to those questions. The only answer the consultation could produce, on its own terms, would be blind acceptance of the document's proposals; all the important issues have been taken as assumptions, not up for discussion or debate.

The bias is clear from the very first words of the document: "Lawful access". Intrusion into Canadians' communication is referred to throughout the document by that slanted name. Claiming that the "access" is acceptable then becomes a tautology: of course something that is "lawful" must be acceptable, that is practically the definition of the word. It would be better to take a step back and consider carefully whether "access" to private communications is ever "lawful", and if it is, under what circumstances it is or is not "lawful". I am aware that the term "lawful access" was not coined for this discussion but is the long-standing term for similar interception of other communications; that begs the questions of whether and how Internet communications are comparable to other communications.

Similar assumptions are visible in the basic structure of the document. For instance, on page 6, the rationale for the proposals is described as a set of three "needs": to update the law for new technology, to allow law enforcement agencies to tap communications, and to ratify the Council of Europe *Convention on Cyber-Crime*. Those are not "needs"; or at least, anyone who claims that they are "needs" had better have a good argument to support it.

It is not obvious that the law needs to change; maybe our current laws are already workable. It is not obvious that law enforcers need to tap communications; maybe they can already do their jobs fine in the current state of affairs. It is not obvious that we need to ratify the Council of Europe *Convention*; it is possible that maybe the Sun would still continue to rise each morning without Canada's ratification

of that document. Those three items are actually important issues for debate, and it is terribly disappointing that the consultation process takes them for granted. It's like saying: "Let's play hockey! First, we'll agree that the final score will be five to three for my team, okay? Now, drop the puck and we'll get started." Why should anyone bother playing the game on those terms?

## **Unsupported technical assumptions**

The consultation document is also rife with unsupported assumptions on specific technical points. I will highlight just one especially worrisome incorrect assumption: the claim on page 12 that an Internet address has a "lower expectation of privacy" than the contents of an Internet transmission; the consultation document seems to suggest that an IP address is close to the category described later on the page of "subscriber" information that "does not tend to reveal intimate details about [an Internet user's] lifestyle and personal choices". That is absurd. The IP addresses a user connects to reveal a great deal about the content of the communication, because an IP address often associates with just one Web site and a Web site often has just one topic.

Suppose we have information that Mr. S, a prominent member of a socially-conservative religious group, connected to the IP address 216.130.177.114 on a daily basis over the course of several months. That sounds like perfectly innocuous information over which Mr. S would have little or no "expectation of privacy": the IP address is just a series of apparently-meaningless numbers.

But anyone on the Internet can turn that IP address into a URL, "http://216.130.177.114/", and type that URL into a Web browser. Someone who did so would find themselves connected to the front page of a site styling itself "All Gay All Day - All the free gay porn you want!". There is no other subject matter available from that particular site -

s.19(1)

communication available through the IP address 216.130.177.114 appears to be more or less as advertised: homosexual pornography only.

Do the authors of the consultation document seriously expect me to believe that Mr. S would have a low expectation of privacy for his connections to that IP address? Do they really believe that the history of his connections to "All Gay All Day" "does not tend to reveal intimate details of [Mr. S's] lifestyle and personal choices"? Would Mr. S be happy to have the log of his accesses to IP address 216.130.177.114, even with no data on specific pages viewed there, published or available to his opponents?

I emphasise that this kind of situation is the norm: the IP address usually allows an observer to accurately guess most of the subject matter of a Web transaction. Furthermore, because people often access the Internet from their own, private, computer systems in the privacy of their own homes, they generally feel their their Web transactions are private. Viewing documents on the Web is much different from, for instance, being seen entering a public bookstore or library and reading a book in front of countless passers-by.

It is nobody's business what Web sites Mr. S wants to visit or what he wants to read or look at having visited those sites. The IP addresses of sites he connects to reveal almost the entire story of his choices in Web viewing material; specific page information pales by comparison. An extremely high standard must then be satisfied in order to justify collection of or "access" to the IP address information, even with specific page information excluded. The situation is much different from that of telephone records, where the telephone number called does not usually reveal much about which person at that address was called, or what was said in the conversation. Human beings talking on the telephone may talk about

anything; a Web server at a given IP address often has only one subject on which it will dispense information. IP addresses, accordingly, have a high expectation of privacy.

## Implementation problems

The consultation document appears to assume that all Internet Service Providers are commercial operations. That assumption is not true at present, but it would become self-fulfilling because the proposals would make non-commercial systems unworkable. At present, Internet access is provided to the public by many non-commercial and non-profit organisations and by individuals. Non-profit community networks like the National Capital Freenet allow members of the public to use the Internet cheaply or for free. Educational organisations like universities provide Internet access to their students. Individuals share their connections within their families, or through hobbyist "bulletin board systems" and public wireless projects.

If non-profit Internet service providers incurred "lawful access" obligations, they would be forced to shut down. Even something as lightweight as a registration requirement, with no fee or other obligations, would destroy the smallest projects. If obligations to collect and store data were enforced, the extra equipment and software for that, to say nothing of staff support, would bankrupt larger non-profits.

There are also technical problems beyond the mere resource problems. A regime of adding interception software or hardware to ISP systems would require each ISP's systems to be compatible with the added software or hardware. What happens if the government-provided software runs only on the Microsoft Windows operating system, for instance? Many ISPs use other systems, for pricing advantages or because their business goals require technical capabilities not provided by Windows. Would

s.19(1)

they be forced to switch, even if that destroys their business because the Windows systems do not support necessary features? Adding interception to telephone systems is challenging, but possible at all only because all telephone systems are technically similar. All computer systems are not technically similar, certainly not to the point of running each other's software. Adding interception capability in a cross-platform way is close to impossible.

There are legal issues for implementation of "access" as well. The consultation document casually suggests that searches under warrant (or warrant-like "production order") could be made less intrusive by allowing the ISP staff to make the search instead of requiring a police officer to be present. That might indeed make the search more efficient and less intrusive - because there would be less risk of the police officer accidentally seeing and seizing something they had no legal justification to see or seize, and the ISP staff member being more familiar with the systems could go directly to the information instead of wasting time searching unrelated sections of the operation.

But shifting the responsibility to the ISP could just as easily have the opposite effect. Police officers are trained professionals, supposedly qualified to conduct searches in a manner that respects the law and the rights of the parties being investigated and innocent bystanders. ISP staff have no such training and we cannot expect them to be trained to the level of police officers in the subtleties of lawful search. That fact throws the entire process based on the results into a bad light: because how can we trust that the information from the search is really correct? An ISP staff member could, and we should expect that they normally would, through no fault of their own include the wrong material in the packet returned from the search, or fail to include something that should have been included. Interpreting what is and is not relevant to an investigation is a difficult task. We should not be placing a police

officer's responsibility on an ISP staff member without police supervision.

I believe the suggestion stems from a concern of technical competence: ISP staff know their own systems and could be expected to be able to find things, whereas police would have to be trained not only on computers in general but on every unique ISP system in particular, in order to conduct a meaningful search. But the fact that police officers lack technical competence cannot be used as an excuse for shifting their responsibilities to ISP staff who lack legal authority. We should instead be making sure our police have the tools to gain technical competence, and we should be paying for that from the police budget instead of shifting the expense to the ISPs; but even before that stage, we should first be taking a hard look at the necessity of doing such searches at all.

## Possession of "devices"

The section on computer "viruses" is included in the document just as if it related to "access", but it actually raises a completely separate set of issues. We can probably all agree that for people to deliberately harm others' data by spreading destructive software should be a punishable offence. But the consultation document, in the space of just three paragraphs, raises huge issues of property rights and freedom of expression without even noting the human rights implications of its proposal.

Computer programs are a form of expression written in a computer language - and "viruses" are computer programs. Although the *Convention* refers to "devices", the consultation document makes clear that that word is taken to include software as well as hardware; it includes expression. Freedom of expression is a basic human right that we cannot suspend lightly.

There are many legitimate reasons (including research and

education) why someone might need to "possess" a computer "virus". For a start, manufacturers of anti-"virus" software cannot be expected to design working products without having real "viruses" to test. But the reasons for possessing a virus should not even be a consideration: computer "viruses" are Constitutionally protected expression and their possession cannot be banned in a democracy. Use of destructive code to harm others' data can be banned; but mere possession of potentially destructive code is harmless - and often beneficial, for its research and educational value.

There is also a serious issue of defining destructive code, and that is one reason I prefer the term "destructive code" to the more nebulous "virus". Destructive code would appear to be software code that causes destruction of data - but how far into hypothesis does that extend? The basic operating system of a computer can be used to delete files, with or without the permission of the computer's owner; does that make it destructive code or a "virus"? Probably not. But what about a piece of software that deletes files without making it clear that that is its function - is that an evil "virus", or might it be merely a product with a confusing user manual? Precise and correct definitions are not so easy to find as they might appear at first glance.

The consultation document uses some qualifying phrases, such as "possession . . . for the purpose of committing a computer offence", which appear intended to allay concerns like mine over the inappropriate reach of a possession offence. But the document also negates that qualification by suggesting in the very same paragraph that new offences would apply "whether or not the virus has been deployed or has caused any form of mischief" - boldly trampling the legal principle that persons cannot be prosecuted in advance for crimes they only *might* commit. That suggestion is hardly reassuring to a free-expression advocate. Throughout any discussion of prohibition on "viruses" or any other form of expression, the issues of the



s.19(1)

human right to freedom of expression, and of prosecution for actual harm, not hypothetical harm, must be paramount.

## Conclusions

In conclusion, then, I have highlighted some of the inappropriate assumptions in the consultation document. I have discussed the horrific consequences for non-profit ISPs of any regime that would impose new obligations on them - even apparently non-intrusive obligations like a registration or licensing scheme. Incautious creation of new warrants and warrant-like powers to be executed without police supervision, would raise serious issues of due process. Finally, although it really has little or nothing to do with "access" and requires a detailed analysis, the consultation document mentions only briefly a proposed new offence for "possession" of intangible software "devices" - which are protected as expression under the Constitution. I am concerned about any such new offence.

Pierlot, Paul

From: [REDACTED] s.19(1)  
Sent: 2002 Dec 16 12:37 AM  
To: la-al@justice.gc.ca  
Subject: LAWFUL ACCESS CONSULTATION SUBMISSION



LAWFUL ACCESS  
SUBMISSION.doc

attached please find my submission to the consultation process.  
please confirm receipt.

yours very truly,

ian

--  
. . . . > ((( (°> . . . . > ((( (°> . . . . > ((( (°> . . . . > ((( (°>

[REDACTED]  
Faculty of Law : Faculte de droit  
Common Law Section : Section Common Law  
University of Ottawa : Universite d' Ottawa  
57 Louis Pasteur St., P.O. Box 450, Stn.A  
Ottawa, Ontario K1N 6N5

[REDACTED]  
. . . . > ((( (°> . . . . > ((( (°> . . . . > ((( (°> . . . . > ((( (°>

# Université d'Ottawa University of Ottawa

Faculté de droit Faculty of Law  
Section de common law Common Law Section  
57, rue Louis-Pasteur 57 Louis Pasteur  
Ottawa ON K1N 6N5 Canada Ottawa ON K1N 6N5 Canada  
(613) 562-5794 Téléc. Fax (613) 562-5124

s.19(1)

The Honourable Martin Cauchon, Minister of Justice and the Attorney General of Canada  
284 Wellington Street  
Ottawa, Ontario, Canada, K1A 0H8

The Honourable Wayne Easter, Solicitor General of Canada  
340 Laurier Avenue West  
Ottawa, Ontario, Canada, K1A 0P8

The Honourable Allan Rock, Minister of Industry  
235 Queen Street  
Ottawa, Ontario, Canada, K1A 0H5

Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor, 284 Wellington Street  
Ottawa, Ontario, Canada, K1A 0H8

December 16, 2002

Dear Mr. Cauchon, Mr. Easter and Mr. Rock:

I am writing this letter in response to your invitation for comments on the lawful access agenda, as set out in your "Lawful Access Consultation Document" of August 25, 2002.

As holder of the Canada Research Chair in Ethics, Law & Technology, I must begin my submission by expressing my very deep concern about the social implications of the current approach of the lawful access agenda in general, and the August 25, 2002 Consultation Document in particular. While the desire to modernize the capabilities of law enforcement and national security agencies is laudable, as is the desire to bring the law into accordance with the current state of telecommunications technology, the proposed means of doing so set out in the Consultation Document, in my view, are not particularly well-measured. In fact, various defects in the Consultation Document make it quite difficult to comment on in any meaningful way.

My submissions are therefore limited to an elaboration of five general remarks. Rather than supply superficial answers to the laundry list of questions raised in the Consultation Document, my aim is to convince those responsible for this process that it is necessary to undertake further study of the foundational issues prior to the completion of the consultation process. Before seeking advice from stakeholders about *how to implement a regime* that could fundamentally alter the relationship between the public and private sector and turn the internet and other converging telecommunications media into a global surveillance system, it is important to have a deeper understanding of the social implications of building it in the first place.

## **1. Lack of Government Disclosure About the Lawful Access Agenda**

Upon reading and rereading the Consultation Document, I was struck by the government's lack of disclosure regarding its legislative plans and by the vagueness that pervaded the various sections of the Consultation Document. Among other things, it was unclear just how closely Canada intends to mirror the approach adopted in the European Convention on Cybercrime. Much to my surprise, many important aspects of the European Convention are not even mentioned in the Consultation Document. Those that are addressed are veiled in generalities, ambiguities and question marks. Attending a public forum on the lawful access agenda that was held at the Department of Justice, Ottawa, on October 21, 2002, I had hoped that the government would finally be in a position to further elaborate on its plans. It did not.

The purpose of a consultation process is to gain useful feedback from the various stakeholders and to use that feedback to shape better legislation. The success of such a process requires full and frank disclosure of what the government intends to do. The Lawful Access Consultation process has not, in my view, proceeded in this manner. Without first disclosing to all stakeholders, with some clarity and rigour, what it intends to do and the perceived implications of so doing, the government cannot hope to carry out a successful consultation. To the extent that the Lawful Access Consultation is deficient in this regard, this will make it extremely difficult to meet the government's stated goal of creating "effective measures that balance the rights, privacy, safety, security and economic well being of all Canadians."

## **2. Presuming Media Neutrality Is Unjustified**

According to the Consultation Document, "[t]he central tenet of the proposal is that service providers would be required to have the technical entirety of a specific telecommunication transmitted over their facilities, subject to a lawful authority to intercept. This would include the content and the telecommunications-associated specific data associated with that telecommunication."

Such a requirement already exists for wire-line telephones and paper-based mail. In essence, the aim of the central tenet is to achieve *media neutrality*, i.e., to extend this requirement to wireless communications devices and the internet so that all media of communication are treated in exactly the same way.

But why should we simply assume that interception/search and seizure standards ought to maintain the *status quo* in digital environments? The ability to intercept networked electronic communications must be seen as accompanied by an inexpensive means of storing, searching, correlating, collating and copying those communications and then recombining the digital information collected through data-mining techniques in a manner that allows the assembly of an

extensive database that would yield revealing and invasive personal profiles. The danger of misuse associated with the interception of digital information could well be qualitatively and quantitatively different than its paper-based and wire-line intercept corollaries. Consequently, there is a need for a much fuller examination and justification of the basis for treating these communications media as though they are the same.

Briefly put, what is most problematic about the central tenet of the lawful access agenda is the fallacious leap from the premises:

**i) lawful access is important, and**

**ii) lawful access currently justifies an intercept capability for paper-based and wire-line communications,**

to the conclusion that:

**iii) lawful access justifies a global intercept capability for all communication media.**

Even if one were to accept that premises i) and ii) are true, the conclusion is not logically entailed by the conjunction of these two premises. At best, the syllogism represents an inductive argument that requires proof based on convincing empirical evidence. Unfortunately, no such evidence is put forth in the Consultation Document. Like the media neutrality principle from which it derives, the central tenet is simply presumed as an article of faith.

The chief difficulty in accepting the central tenet on faith is that it is clearly problematic from a privacy perspective. A legal regime that mandates a global intercept capability teeters on the brink of creating a panoptic society of the sort that Bentham dreamed about and Foucault understood only too well. As Foucault has told us, the nature of panoptic power is bound up in the possibility that the exercise of such power is visible yet unverifiable. Those who live within the panopticon cannot see those who might be watching, but are forced to live with a constant awareness that someone could be watching at any moment. Through the exercise of panoptic power, citizens never know for sure whether or when they are actually under surveillance. Such a power structure – which is premised on a lack of transparency – is antithetical to a free and democratic society. Compliance and subordination are achieved not through the development of laws or moral rules but through the creation of uncertainty and a general loss of privacy. Such a power structure assures that, in Foucault's words, "surveillance is permanent in its effects, even if discontinuous in its action." These conditions lock those within in "a state of conscious and permanent visibility that assures the automatic functioning of power."

Has the Consultation Document demonstrated that law enforcement's need for access justifies the exercise of such extraordinary power?

I would submit that it has not. The decision to mandate a global intercept capability is not simply the logical conclusion of lawful access in a digital age. Policy makers must understand that the choice to mandate a global intercept capability is a much more drastic decision with enormous implications on personal autonomy that will impact the ability of individuals to exercise their rights in a free and democratic society.

### **3. Precluding Technological Neutrality Impedes Innovation**

In addition to presuming media neutrality with no demonstrated basis for doing so, the Consultation Document mistakenly ignores an important corollary principle: the doctrine of technological neutrality. Technological neutrality recommends that regulatory regimes avoid reference to specific states of technology. This doctrine reflects the fact that technical standards

change rapidly. It recognizes that legislative standards created with specific technologies in mind are likely to become outdated when those technologies evolve.

Among other things, the Consultation Document suggests that a global intercept capability would be built pursuant to the government's authority to set technical and other standards. The Consultation Document even indicates the possibility of mandating the specific type of apparatus that service providers must install as well as the exact capacity requirements of their intercept capabilities.

By precluding the possibility of technological neutrality, the legislative scheme for lawful access would likely be cumbersome and inefficient. Each time a new innovation is adopted in the market, policy makers would be forced to consider legislative or regulatory amendments. Alternatively, by forcing service providers and other technology industries to adhere to particular technical standards in spite of new technological developments, lawful access legislation could very well impede the development of innovation in Canada and abroad. It should be remembered that the internet's infrastructure was founded upon a principle of openness. Originally, the internet's developers were its users. Standards were developed only as the need arose. If the particular technical standard worked, it was shared with everyone and adopted by the community as a whole. If it did not, it was quickly forgotten. The imposition of technical standards by government would drastically change the culture of innovation and would therefore be unwelcome, especially by innovators from other jurisdictions.

#### **4. Encryption Technologies Render Intercepted Information Ineffectual**

The ability to intercept electronic communications might be a necessary condition for preventing or solving some cybercrimes, but it is certainly not a sufficient one. An important criticism of the global intercept requirement is that, in spite of the level of invasiveness it could have on the general population, it would be ineffective on its own as a means of investigating those engaged in organized crime.

Effective investigations require, after all, that law enforcement agencies are capable of understanding intercepted communications. Sophisticated criminals could circumvent this possibility through the use of various encryption technologies. For criminals or others who have an incentive to use encryption for some illicit end, such technologies are readily available and present a fairly secure means of maintaining secrecy in spite of an interception capability. Thus, one practical effect of the call for a global intercept capability is that criminals, terrorists, and the tiny minority of others who use encryption for all networked communications will be the only ones who are guaranteed privacy online.

#### **5. The Proposed Lawful Access Regime Undermines Service Providers' Relationships With the Public**

Wireless, wire-line and internet service providers do more than just provide the means of communication. Many provide storage, retrieval and numerous other information management services. Up until now, most service providers have self-defined as the stewards of our personal information and private communications and the guardians of informational privacy. As we move further into networked environments – with an increasing tendency to remove information management capabilities from individual users, placing them within the sole control of network operators and servers – our dependence on service providers to safeguard our personal

information and private communications will only escalate. Each of us is dependent on these service providers not only for the proper storage, maintenance and management of our personal information, but also for ensuring that our private communications are secure from intrusion and kept confidential.

It is important to recognize that once our personal information falls into the care and control of a service provider, we become vulnerable. Having placed our trust in them, we are at the mercy of their discretion. Thus, in many instances, our service providers are fiduciaries. The leeway that we afford to service providers to affect our legal positions (by allowing them to decide what of our personal information to disclose and to whom) puts them in a position of power over us. They have the power to regulate our behaviour and to alter the fate of our personal outcomes.

The lawful access agenda calls for various changes that could undermine the delicate relationship of trust between service providers and the public. The Consultation Document's proposed requirements to preserve, produce or disclose our personal information and private communications (and to generally facilitate law enforcement investigations, in some cases on an expedited legal standard lower than that which is currently required by law) undermines the role of the service provider as a trusted information intermediary.

Traditionally, the dominant metaphor for the relationship between service providers and the public has been that of an *information conduit*. When legal proceedings arise, service providers have, until now, been quite successful at avoiding criminal and civil liability on the basis that they are merely the pipeline that runs between those in communication. The lawful access agenda radically changes this. Service providers can no longer function as trusted information intermediaries who owe a duty of loyalty to their subscribers. Nor can they be said to act as a mere conduit for communication. If implemented, several proposals within the Consultation Document would transform the service provider into an *information reservoir*. As such, service providers would likely become the richest repository of investigatory information.

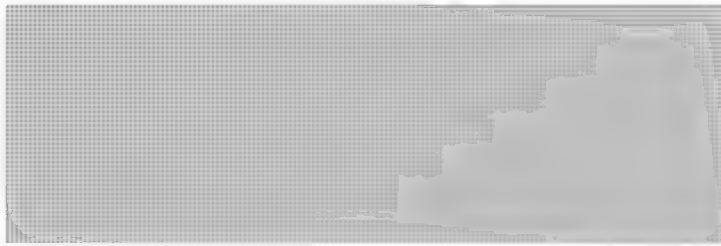
Many difficulties arise when a service provider is made to function as an information reservoir. For example, criminal investigations, which have traditionally been understood as a public sector activities, will come to rely more and more on private sector participation. This blurring of the line between public and private has obvious constitutional law ramifications. Are private sector service providers agents of the state? Is information that is collected by a private sector service provider subject to the unreasonable search and seizure provisions in the *Charter of Rights and Freedoms*? None of these considerations are addressed in the consultation document.

## Conclusion

The aim of this submission has been to demonstrate that there is a need to undertake further study of the foundational issues prior to completing the consultation process that is currently underway with the various stakeholders.

It is my sincerest hope that those charged with the oversight of this process will recognize the need for further study and, accordingly, extend the consultation period to include additional phases that integrate a continued examination of these foundational issues. Only after gaining a deeper understanding of the social implications of adopting such a regime, can a meaningful consultation take place on the details about how best to implement it.

Yours very truly,



s.19(1)



Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 16 12:45 AM  
To: la-al@justice.gc.ca  
Cc: [REDACTED]  
Subject: Lawful Access submission



Lawful Access.doc

Please find attached my submission to the consultation process on Lawful Access.  
Note that this paper is copied to [REDACTED] for archival on his website.

Sincerely,

[REDACTED]  
New Westminster, BC

I am a software developer with over ten years experience in the industry, commenting as a Canadian citizen. I would like to thank the Department of Justice, Industry Canada and the Solicitor General of Canada for the opportunity to provide input on these proposals.

## **Overall Comments**

The Consultation Document talks of the Internet as having "created difficulties for investigators" but does not provide any details of, or evidence for, these "difficulties", which makes it a little difficult to provide useful input. In addition, at least as far as the Internet is concerned, the "need for sophisticated equipment" would appear to refer to little more than packet sniffers, which are widely available for a cost of a few thousand dollars.

The Consultation Document discusses the Council of Europe Convention on cyber-crime. It states that as of August 2002, 33 countries had signed the convention, but does not mention how many have ratified it. It then talks about "the need for Canada to adopt statutory measures that will permit ratification of [the convention]". I am very concerned that international treaties such as this are signed with no democratic consultation process and then presented to the electorate as though it is essential that we ratify them. If ratifying this, or any other international treaty or convention means giving up significant freedoms, then clearly it should not be ratified and whoever signed it on Canada's behalf should be disciplined.

I immigrated to Canada from England 7 years ago because I saw that the government there was tending to control and mistrust the population rather than to serve it. I want to live in a true democracy where the right to communicate privately is recognized as an essential part of the democratic process and where it is recognized that security should never be increased if doing so means restricting the freedoms that make us a democracy. When the Privacy Commissioner of Canada condemns proposals, they should immediately be withdrawn.

## **Infrastructure Capability**

I have two main problems with the proposals in this section – (1) they seem to be a very expensive way of doing things and (2) at least for the internet, they don't achieve the objective.

I am going to concentrate primarily on the Internet side of things because that is the area I am most familiar with. Here, there are many very small service providers, the service providers are not generally very profitable, the service provided is regarded by the government as being very important and end-to-end encryption is readily available and widely used. If these proposals were to be enacted, many Internet Service Providers [ISPs] would go out of business due to the increased expense, the remainder would pass the costs on to their customers, making access to the Internet more expensive and thus available to fewer people. Then we have the ability to intercept Internet communications anywhere in Canada, to a far greater degree than we now have the ability to intercept postal mail. Presumably the majority of this interception capability would then sit idle for the majority of the time. There is, of course, the risk of illegal use of this capability, which is not a concern if the capability is not mandated to be present. When it is used legally, it is quite likely that the intercepted communication will be encrypted, which will take significant time and money to break, if doing so is even feasible. Deliberately adding

call and websites they visit, would consider their Internet use more private and prefer to publicise their use of the telephone. The Internet is used to access support websites for diseases or lifestyle choices, for shopping, banking and even to listen to music and read books. A person's use of the Internet tends to reveal very intimate details about their lifestyle. Most Internet users believe that they can remain anonymous if they so choose – the frequency of “flame wars” on the Internet has been attributed to the perceived lack of accountability for one's action son the Internet. While I agree that in reality it is far easier for Internet transactions to be intercepted by a third party, this does not affect the **expectation** of privacy – most Internet users believe, perhaps wrongly, that their use of the Internet is more private than their use of the postal service and more anonymous than their use of the telephone. Any legislation directed at the Internet must take this into account.

### **Specific Production Orders**

The important point here is that an Internet Protocol address, although it may be analogous to a telephone number in that it identifies a single destination for a communication, should not necessarily be subject to the same level of protection as a dialled telephone number. As mentioned above, Internet users tend to have a higher expectation of privacy for their use of the Internet than they do for the telephone. Also, an Internet user tends to access many more destinations (for example, websites) in a given period of time than a telephone user will dial telephone numbers. Many website visits are very brief, and it is far easier to move from one website to another than from one telephone number to another. It is also worth mentioning here that email headers tend to reveal much more information about a communication than the postal equivalent. Email headers typically include not just the addressee but also the source, subject and size of the message.

### **Orders to Obtain Subscriber Information**

The Consultation Paper makes it clear that Orders to Obtain subscriber Information are only really desired to allow law enforcement agencies to conduct “fishing expeditions” where there is insufficient justification to make a court order obtainable. The criteria required to obtain a court order have been established over a significant period of time to balance the privacy rights of Canadians against the needs of law enforcement. If there is insufficient justification for a court order, the privacy rights of the individual are more important than the desires of law enforcement. This balance that has been established over a period of many years should not be disturbed just because doing so would make the job of law enforcement easier. If that logic were to be accepted, we would all be subjected to periodic searches of our homes and persons.

If court orders are truly too difficult to obtain (which I doubt), the better solution would be to make them easier to obtain, not to allow law enforcement to avoid them completely. Judicial oversight is essential if law enforcement is to be perceived as serving, rather than oppressing, Canadians.

### **Data Preservation Orders**

The Consultation Paper discusses preservation “for only as long as it takes law enforcement to obtain a judicial warrant”, then suggests that a reasonable period might be

## **Access to Hidden Records**

This sounds very much like it would violate the principle that people cannot be required to incriminate themselves.

## **Other Mechanisms to Provide Subscriber Information**

A national database ? Please. This would be impossible to keep accurate, a violation of privacy, a very tempting target for criminals and almost certainly abused by its maintainers.

Service Providers should absolutely not be compelled to collect any information that they would not normally collect, under any circumstances. This could destroy legitimate business models that rely on not collecting such information, add costs (especially as the Service Provider will have to comply with PIPEDA) and offloads work that law enforcement agencies should be doing onto Canadian businesses.

## **Conclusion**

Since our own espionage agencies, which are not subject to the same checks and balances as law enforcement, are now permitted to spy within Canada, it is more important than ever to ensure that the privacy of Canadians, the ability to freely communicate, and the *perception* of the ability to freely communicate are protected. I hope that any changes made as a result of this consultation will recognize this.

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 16 8:49 AM  
To: la-al@justice.gc.ca  
Subject: Submission on Lawful Access

s.19(1)



CAC-ITS Submission  
Lawful Acce...

Please find attached the submission of our standards committee, comments on the Department of Justice Lawful Access Consultation paper.

The CAC-ITS is a voluntary standards committee, operating under the mandate of the Standards Council of Canada, that contributes to national and international standards on information technology security. The CAC-ITS is the National Body representative to the International Standards Organization (ISO)/ International Electro-technical Commission (IEC), Joint Technical Committee, sub-committee # 27 on IT security techniques.

Please feel free to contact me should you have any questions about our submission.

We appreciate the opportunity to comment on this important initiative.

Thank you,

[REDACTED]  
Canadian Advisory Committee - Information Technology Security  
ISO/IEC JTC1 SC 27  
Phone: 613-232-2350  
[REDACTED]

## **Canadian Advisory Committee – Information Technology Security ISO/IEC JTC 1/Sub-committee 27 – IT security**

### **Comments on the Department of Justice Lawful Access Consultation Document dated August 25, 2002**

#### Introduction

We offer these comments from the perspective of the mandate of our ISO/IEC Sub-committee, and our role as Canadian Advisory Committee for the development of Information Technology Security (ITS) national and international standards.

SC 27 is responsible for the standardization of generic methods and techniques for IT security. This includes:

- identification of generic requirements (including requirements methodology) for IT system security services;
- development of security techniques and mechanisms (including registration procedures and relationships of security components);
- development of security guidelines (e.g., interpretive documents, security risk management), and
- development of management support documentation and standards (e.g., terminology and security evaluation criteria).

In view of the scope of our standardization committee, then, we are keenly interested in the development of the Canadian lawful access legislation, and pursuant regulations and standards. We offer the following comments in that context.

#### General

In principle, the concept of lawful access is fundamental to the protection of the right of our citizens to safety and security, and to the protection of our government institutions and critical infrastructure. There are circumstances under which it is entirely appropriate and necessary for law enforcement and security and intelligence agencies to intercept network based communications of persons suspected of wrongdoing; the increased visibility of law enforcement responsibilities since 9/11 neither increases nor diminishes this fact. This fact, however, must be balanced with the right to privacy in our democratic society. This of course includes the privacy of communications, and the bulk of network traffic is benign private communication.

Some of the provisions of the lawful access consultation paper raise concerns with respect to private and benign communications. There are also potentially significant implementation issues that need to be considered. Our comments address those concerns, while, at the same time, recognizing the importance of lawful access for the preservation of our overall freedom.

The purpose of the consultation paper is to provide concerned stakeholders with an opportunity to consider proposals to update Canada's lawful access provisions. The proposals address requirements stemming from three primary needs:

Following on from the above comment, the paper makes reference to a "private document", but does not actually define what constitutes a private document. From the discussion related to the intercept of e-mail, it is obvious that legal opinion on this matter is divided, with one school of thought being that e-mails should be considered private documents (or private communications – is this the same thing?) and with the other suggesting that putting any communication in writing renders it non-private (does this line of reasoning also apply to conventional "snail mail"?). There is also no discussion of the implications of using cryptography or other means for concealing/protecting the contents of network traffic and subsequently increasing the expectation of privacy (see related provisions in the *Criminal Code* in this respect).

### Real-time monitoring

The paper suggests that amendments could be made to other existing laws (e.g. the *Competition Act*) in order to modernize them in accordance with the *Convention*, notably in the areas of real-time tracing of traffic data and the interception of e-mail. Real-time tracing of network traffic is exceptionally difficult, particularly if the "intruder" has taken steps to disguise the source of the traffic, or if the traffic is of short duration.

Real-time tracing requires the identification of the malicious traffic and the identification of upstream service providers through correlation of outbound malicious traffic with inbound malicious traffic. This presumes that upstream providers have the necessary capability to perform this correlation, and that they are prepared to cooperate in the tracking of the malicious traffic. This presumption is faulty in most instances, and particularly in the case of small ISPs or those that offer anonymous services, respectively. Limited cooperation already takes place amongst service providers, usually in response to a customer complaint.

Setting aside these difficulties, the real-time tracing of traffic still requires intercept of the traffic. Will judicial authorization be required for this interception? If so, will the same standards apply as for more traditional intercept of telecommunications?

The consultation paper refers to an "anticipatory order" which would permit law enforcement agencies to monitor transactions for a specified period of time (as an issue to be considered). It is difficult to comment on such a proposal in the absence of any discussion of the standard required or the circumstances under which such orders would be authorized. On the basis of what little information is provided, these could be misinterpreted as "fishing expeditions". There is also no discussion as to how long an "anticipatory order" could be in effect (i.e. 24 hours, 7 days, or some other period).

### Production and Preservation

The paper discusses production and preservation orders. A production order requires disclosure of documents and records that already exist (that have been created in the normal course of business); a preservation order requires that any such document or record not be routinely destroyed.

The paper describes the type of information that might be subject to a production order, which in turn assumes that such information is routinely retained by telecommunications service providers (TSPs). The information is variously defined as telecommunications-associated or traffic data.

According to a Government of Canada document entitled Data Preservation Checklists (available at <http://www.g8j-i.ca/english/doc4>):

"data preservation does not compel either collection or retention of data; it is essentially a "do-not-delete" order pertaining to existing data. A data preservation scheme provides that upon a lawfully authorized request, based on the facts of specific case, particular data that has already been collected can be preserved to prevent its deletion. At a later point, a lawful request by a competent authority can compel disclosure of the data."

While a data preservation scheme may "not compel either collection or retention", it presumes that this is in fact taking place: in the absence of collection and retention, there will be no data to preserve. As noted above, there may be very little business requirement for ISPs to collect or retain traffic data, and in some cases, they may not have the technical capability or capacity to collect and retain data over a sufficiently long period of time to adequately support tracing of communications.

The imposition of any form of data retention scheme on TSPs will create significant practical difficulties. Even the retention of traffic data only could result in the requirement to store large volumes of data, which in turn creates the following problems:

- data storage (i.e. what media to use),
- data management (e.g., how to index it in such a way as to permit later retrieval in response to a production order), and
- data protection (e.g., to preserve its admissibility in court, by protecting against media deterioration and preserving the chain of custody).

The paper asks the question: "What is a reasonable period for a custodian to be compelled to preserve data: 90, 120, 180 days?" The assumptions for the purposes of this comment are that preservation will only involve a limited amount of traffic (i.e. traffic related to a limited number of persons), and that preservation will only commence as of the time the preservation order is served on the TSP (preservation of data prior to that point would in fact be data retention, or would be in response to an anticipatory order).

The amount of data to be preserved would depend what was being preserved (i.e. traffic data only, or traffic and content data), on the number of communications to be preserved and the duration of preservation. There are no clear guidelines for recommending a particular retention duration, as it is dependent upon a number of factors, each of which can vary considerably. Factors include: why the data is being preserved; how long it will take for an investigation and any follow-on action, such as prosecution, to be completed (the preserved information presumably being an element of the investigation); how long after these events the evidence must be retained (which could be, for example, until all appeals have been exhausted).

#### Costs

The paper outlines when service providers would bear the costs of ensuring that intercept capability is built into their facilities:

- for new technologies and services;
- for significant upgrades to systems and networks; but



collecting the information for its own purposes, then no obligation should be imposed to routinely collect it strictly for law enforcement purposes). This should not preclude the collection and preservation of the information in response to a duly authorized judicial order – but the mechanism to do this would not be a preservation order (a wiretap order instead?).


The paper suggests that a national database of customer name and address information and local service provider identification information could be developed and implemented to facilitate law enforcement and national security agency access to such information. The paper does not discuss the requirements for such a database, nor does it provide compelling arguments for its creation. Given the controversy over the HRDC databases of a few years ago, any such move will likely spark considerable outrage on the part of the average citizen (even allowing for the possibility of increased tolerance post 9/11, any such tolerance will have worn thin by now).

### Conclusion and Recommendations

It is important for both public and private sectors in Canada that we maintain our interoperability and consistency with related initiatives in allied nations and in regional organizations (i.e. EU). We recommend, therefore, that the Department of Justice continue to consult with their counterparts amongst our allies, to ensure that whatever final direction we take in lawful access, we will still be competitive internationally and we will still be able to share intelligence information with our allies.

The Department of Justice consultation document recognizes the importance of maintaining a level playing field for all stakeholders. The impact of the proposals in the document will be felt most onerously by the Canadian SMEs that provide ISP and related services. We recommend, therefore, that the government undertake to fund the necessary technological changes required for compliance to the provisions of any lawful access legislation and pursuant regulations.

s.19(1)

  
Canadian Advisory Committee - Information Technology Security  
ISO/IEC JTC1 SC 27

Pierlot, Paul

s. 19(1)

From: [REDACTED]  
Sent: 2002 Dec 16 11:10 AM  
To: la-al@justice.gc.ca  
Cc: "Bélanger, Mauril - M.P."  
Subject: Lawful Access submission from [REDACTED]

(Note: I am copying this to my MP, Mauril Bélanger)

The following is my submission to the Lawful Access consultation.

[REDACTED]

Please confirm that you received this document. If I need to send this in another format, please let me know so that I can convert and re-submit.

Please let me know if a full list of submissions will be published online, and what the location will be. Please do reference or re-publish this document as appropriate.

---  
[REDACTED] Internet Consultant: <<http://www.flora.ca/>>  
Any 'hardware assist' for communications, whether it be eye-glasses, VCR's, or personal computers, must be under the control of the citizen and not a third party. -- [REDACTED]

Homepage Open Systems  
Weblog Network Status



Clients, Associates Services  
Contact Information Rates

s.19(1)

## Lawful Access 2002

This is my submission to Lawful Access consultations (Canadian Department of Justice). Please also see LexInformatica: Cybercrime and Lawful Access.

### Copyright

Copyright (C) 2002, [REDACTED] <<http://www.flora.ca/>>

Permission is granted to reference, republish or include this document in your own materials, in whole or in part, as long as some form of acknowledgment is made. If the new work is a derivative work, please ensure that it is marked as such so that it will not be confused with my own writing.

### Introduction of a Cyber-citizen

I am aware of other submissions that address some of the key legal and technical implementation issues in detail. I will not repeat that discussion here to try to keep this submission as small as possible. Public servants are invited to communicate with me directly for any clarifications relating to this submission, or any other area of law or technical implementation where my perspective would be helpful to the Government of Canada. Much of what this consultation paper is asking the public to offer, even if we as a society wanted to grant it to the police, cannot be implemented in technology as simply as this paper appears to assume.

My submission will be of a more personal nature. While I was born in 1968, I became involved in on-line communications at an early age given the time. Growing up in "cyberspace" has allowed me to see many issues from a vantage point that may be different from the average Canadian.

We are quickly approaching the 20-year anniversary of the birth of the Internet. The most logical date of origin of the Internet is January 1, 1983, when the ARPANET officially switched from the NCP protocol to TCP/IP (letter to CANet-NEWS). My first involvement in electronic communications came the same year, when I became a Sysop (System Operator) for a Bulletin Board System (BBS) running at Science North in Sudbury, as well as a Co-Sysop for a number of other BBS systems. I am currently the sole-proprietor of an Internet based business called FLORA Community Consulting that does a mixture of Free/Libre and Open Source Software (FLOSS) consulting, support and ISP services.

Growing up in this environment, I consider myself a citizen of 'cyberspace' first, a citizen of 'planet earth' second, and only lastly a citizen of Canada. Legally I am only considered a citizen of Canada, but my allegiances are not to the interests of "Canada" any more than any other nation state.

As a citizen of cyberspace, I take to heart the February 8, 1996 "Declaration of Independence of Cyberspace" as published by community leader John Perry Barlow. Where I differ from this declaration is that I do fear the imposition of foreign laws onto cyberspace, which is why I am sending this submission to the Canadian Department of Justice.

As a citizen, I have a strong respect for rule of law and a strong moral code. I am also an active participant in the formation of laws and other public policy, both in Cyberspace and in Canada. I have made many submissions such as this one to the Government of Canada, including a submission to the 2001 copyright reform consultation and the 2002 Innovation Strategy.

### Profiling of the politically active

It is unfortunate, but it is my active involvement in politics which makes me most fearful of Lawful Access. I have read other submissions that discussed the possible defacto-offense of "Surfing while Muslem", discussing how a lack of judicial oversight in cybercrime investigations can lead to biased profiling. As a politically active person, I suspect that I would be one of those citizens that would be targeted for such profiling.

To clarify, it is not my political beliefs around Competition, Copyright, Innovation and Patent policy that would make me a target. While there are special interest groups that strongly disagree with my views in these public policy areas, these are not (as of yet) target areas for police investigations.

Where I do believe I will have problems relate to my beliefs on international courts, international trade, and terrorism. I recently wrote a letter to my Member of Parliament, Mauril Bélanger, on this topic.

It is almost redundant that I send this, but just wanted to ensure that the statistics relating to constituents on this issue included one more person opposed to war on terrorism, and the "Iraq Attack".

I suspect you already know my views, which are based on very strong support for international law. I believe that any country that has not ratified the ICJ (and has been found guilty of crimes by it) should not be allowed to participate in a "war on terrorism". I believe that any country that has not ratified the ICC should not be allowed to send troops to foreign soil, especially under the name of a "war on terrorism".

If the only reason for Canada's involvement is to show solidarity with the USA (which appears to be the only justification offered so far), and the **USA has no legitimate involvement**, then Canada should also have no involvement.

I have read many times that the Lawful Access proposals are far reaching, yet there is little evidence offered that the changes are actually needed by law enforcement. I worry about any lessening in the requirements of "reasonable and probable cause" as my personal political beliefs may make me a target for surveillance "fishing trips".

When the "terrorism" card is played, many people fall into place. There is a belief that the "war on terrorism" justifies such new and administratively simplified (IE: removing some of the otherwise existing checks-and-balances) investigative tools. How I feel about this should be obvious given that my strong belief in international law and international courts has lead me to a different opinion on the "war on terrorism".

I am currently the ISP for a site called Rooting Out Evil. This is a group of citizens who wish people to join them in challenging rogue states run by military fanatics who produce and conceal weapons of mass destruction. The site asks people to become an Honorary Weapons Inspector and support their mission into the USA.

### ISP communities

Unlike in the monopoly based telecommunications industry where only large telephone companies exist, ISPs come in all shapes and sizes. Requiring that ISPs disclose information may put citizens into the uncomfortable position of 'snitching on their neighbor'.

I have a personal relationship with either the owner or many of the staff for each ISP that I am a customer of. As an active member of the local cyber-community, it would be near impossible for me to have a relationship with an ISP that was entirely arms-length.

Requiring 'neighbors' and possibly close friends to divulge private information about each other, even with a full warrant, without telling the friend is highly unethical. When forced to trust a friend/neighbor or law enforcement, it would be extremely hard for me to believe/trust law enforcement.

A society that encourages/mandates that neighbors 'snitch' on each other brings us considerable social problems that may outweigh the social costs associated with the 'crimes' that are being investigated.

### Multiple uses for security/privacy technology

It is important to realize that the technology used to 'secure' citizens from cyber-attacks is the same technology that will 'secure' citizens from wiretap. The technology has no way to differentiate "unlawful access" from "lawful access". The quest to give police powers to "protect" citizens from threats can never be used to justify making citizens less able to protect themselves.

Citizens should be encouraged to use cryptography on their own communications, and to harden/secure any computers that they connect to the Internet. I worry that laws around Lawful Access may eventually be used to justify laws limiting or prohibiting the ability of secure their own communications.

Any tools that are used to "keep criminals out" of the communications and communications tools of law abiding citizens will also "keep law enforcement out". ICT tools can not differentiate circumvention initiated by law enforcement and circumvention initiated by criminals.

The United States has considered cryptography as munitions, and has laws which seek to control the export of cryptography. This foreign law has been a great hindrance to the wider spread adoption of privacy and security tools in Canada, given that producers of technology do not want to have to create a version for different countries.

### Citizen control of technology

I fundamentally believe that citizens should be in control of the Information and Communications tools they use, and not any third party. Any attempt to give 'law enforcement' a back-door into citizens communications tools will become a target for 'unlawful access'.

In the context of 'copyright reform' I made the following two statements that apply equally to issues of privacy and other forms of cyber-security.

Any 'hardware assist' for communications, whether it be eye-glasses, VCR's, or personal computers, must be under the control of the citizen and not a third party.

Corollary: The "content industries", such as the motion picture and recording industries, are not legitimate stakeholders in the discussion of what features should or should not exist in my personal computer or VCR, any more than they are a legitimate stakeholder in the production of my corrective eye-glasses. If a member of a content industry don't like the technology that exists in a given market sector, be it consumer electronics in the home or personal computers, they can simply not offer their products/services into that market.

### Prohibition of 'illegal devices'

The language used in the consultation document under "Virus Dissemination" is all too familiar to our community from "Legal protection for Technological Protection Measures" (Copyright), cryptography export and other such laws. It is my belief that these types of laws tend to backfire against the intention of the laws.

The language used to discuss viruses is very vague. I do not believe it is appropriate to equating software to a "device", given that there are always many legitimate and legal things done with software, even software that when executed for the purpose intended by the author does not have substantial legal purposes. The anti-virus community relies on the importation, reverse-engineering and documenting of viruses in order to protect citizens from the harmful effects of viruses. This is similar to the cryptography community which will attempt to crack all existing cryptography as a required part of research toward more effective cryptography.

There is also the question of what constitutes substantial lawful purposes. We already have obvious cases in the digital copyright field where software developers are seemingly randomly being charged for acts which not only should not be considered legal, but should be protected acts.

Two examples are U.S. v. Sklyarov (a.k.a. US v. Elcomsoft) and Norwegian Motion Picture Association v. Jon Johansen (DeCSS). In both cases these software developers made use of reverse-engineering in order to create compatible tools. This is a protected right in some countries, and is discussed in the European union 1991 directive on computer software.

I already wrote how citizens should be in control of communications tools. Critical to this is the recognition that computer 'interfaces' (between a human and a computer, between software and hardware, or between software components) should not be eligible for any type of government granted (or enforced) exclusivity, whether that be in the form of copyright, patents, or claimed trade secrets.

There is other currently controversial software such as peer-to-peer file sharing utilities which primarily have lawful purposes, but which some special business interest wish to have declared as unlawful.

A tool that may be used for an 'unlawful purpose' should only be used as additional evidence in the investigation of a specific 'unlawful act'. We should not ever be trying to declare multi-purpose software as being 'unlawful'. Software can never know whether it is being executed for lawful or unlawful purposes, only the human being in control of the software can know this.

It should be noted that as more control of communications tools are placed in the hands of citizens, the more immune they are able to make themselves to malicious software such as viruses. I am a strong believer that Free/Libre and Open Source Software (FLOSS), which allows for open public peer review

of software, is inherently more secure against viruses and other forms of attack. On the other hand, some security consultants believe that popular vendors such as Microsoft should be considered criminally negligent due to the design flaws in their software which make virus infections against their software trivial.

## Protection of protest and civil disobedience

Just because something is claimed 'illegal', does not mean that society will agree that it is wrong. We need to be careful creating tools to simplify the investigation of act where the laws that suggest they are crimes may be very temporary or not considered by society as a crime at all. Judicial oversight, various checks and balances, and the requirement for "reasonable and probable cause" would tend to reduce the intensity of investigations into such actions.

April 5th, 1930, Mahatma Gandhi and about 75 followers marched to the sea in what has become known as the "salt march" in India. This was a protest against a claimed salt monopoly by the British government. Most people today do not see this act as being one of a criminal, but one of a hero.

When dealing with some laws being imposed on cyberspace by nation-state governments, such as the excessive monopolization of communication being granted with the expansion of so-called "intellectual property" law, some believe the same will happen in Cyberspace as happened in India.

In a summer 2001 submission to Industry Canada I indicated that I believe that the USA's interpretation of Copyright is wrong in the case of DVD viewing technology, and that what is happening should be understood as a violation of Canadian competition law. I have stated a willingness to disobey interpretations of this law based on my belief that my interpretation is more correct.

## Clarification of jurisdiction for laws affecting the Internet

There have been many cases where the jurisdiction of crimes that happen online have come into question. Most recently I read a press release from Reporters Without Borders (Reporters Sans Frontières) about the case in Australia.

Reporters Without Borders (Reporters Sans Frontières) today voiced deep concern about the Australian high court's ruling yesterday that online publishers can be sued for libel in the countries where they are read and where the plaintiff's reputation is at risk, rather than in the countries where the publication originates. The decision was taken in connection with Australian mining businessman Joseph Gutnick's libel suit over an article published online in August 2000 by the US magazine Barron's, owned by the Dow Jones news group.

A similar discussion happened around the Hague Conference on Private International Law which included articles such as Richard Stallman's "Harm from the Hague".

The basic idea is reasonable enough: if someone hits your car in France or breaks a contract with your French company, you can sue him in France, then bring the judgment to a court in whichever country he lives in (or has assets in) for enforcement.

The treaty becomes a problem when it is extended to distribution of information -- because information now travels normally and predictably to all countries. (The Internet is one way, but not the only way.) The consequence is that you could be sued about the information you distributed under the laws of *\*any\** Hague country, and the judgment would probably be



enforced by your country.

For me this issue is simple: If I cannot, through democratic representation, help change the laws of a country --- nor have I physically decided to visit that country or are doing business in that country --- then I should not be expected to honor (or even be aware of) the laws of that country.

I live in Canada, have Canadian citizenship, and participate very actively in the development of public policy in Canada. I do not live in China, USA, or Afghanistan, and cannot participate in public policy development in those countries. I should be expected to obey the laws of Canada, not the laws of foreign countries which I should not reasonably be expected to even be aware of.

As John Perry Barlow would say, the Internet is both everywhere and nowhere. The people who's ideas are communicated on the Internet live in some specific country and should be expected to obey the laws of that country. They should not be expected to also obey the laws of every other country that happens to have citizens who communicate via the Internet.

### **The louder you ask for something, the less likely you are to get it**

The more visible that Internet wiretapping becomes, the harder it will become to have successful wiretaps. It should be assumed that criminals already make use of privacy enhancing tools. Criminals that are not doing so are likely committing de minimis crime that should not be the subject of wiretap.

Increasing the cost of providing ISP access in order to provide "methods to wiretap" will be impossible to keep secret. Citizens will ask what the increase in costs relate to, and will be told by their ISPs.

Law-abiding citizens noting the attack on their privacy will be more likely to make use of cryptography than in the past. Increased usage of cryptography will make law enforcement interception of messages even more expensive as less and less information will move over the Internet unencrypted.

It needs to be understood that the more that law enforcement tries to make wiretapping administratively easier for them, the technologically harder wiretapping will become. I have had the configuration the IP Security (IPSec) services of [FreeSWAN.org](http://www.freesswan.org) as a plan for some time. The discussion around 'lawful access' had made me bring this to a higher priority for my business and personal communications.

### **Conclusion**

In your introduction, it is stated that "Clearly, it is important to maintain the principle and powers of lawful access. The challenge is to do so in the face of rapid technological change and in a manner consistent with the Canadian Charter of Rights and Freedoms."

I believe that your paper did not demonstrate that new powers are needed, or that there is adequate understanding of the technology involved in order to be consistent with the Canadian Charter of Rights and Freedoms. You speak of ratification of the Council of Europe Convention on Cyber-Crime as something that Canada must do. It may be that the Europeans do not have any better understanding of the technology and should not be followed.

I believe you should get in better contact with the technology community, starting with some of the individual citizens like myself who sent in submissions. A better understanding of the technology involved may allow you to better determine how best to move forward. You may simply determine that no changes at a technological level are necessary or desirable.



---

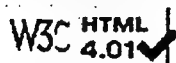
Last update: \$Date: 2002/12/16 21:51:35 \$ UTC

---

The current date/time is Wed Dec 18 13:55:55 EST 2002.

Please note the following information offered to this server by your browser. It is useful to know this information to determine what information a citizen would expect to be reasonably private, compared to the level of information which a website host can actually collect.

HTTP Request Header	Value
Accept	*/*
Accept-Encoding	gzip, deflate
Accept-Language	en-ca
Connection	Keep-Alive
Host	www.flora.ca
User-Agent	Mozilla/4.0 (compatible; MSIE 5.5; Windows 98; T312461)



Pierlot, Paul

---

From: [REDACTED] s.19(1)  
Sent: 2002 Dec 16 11:17 AM  
To: 'la-al@justice.gc.ca'  
Subject: US Internet Service Provider Association's letter on the "Lawful Access"

Dear Sir or Madam,

The attached document contains a response from the US Internet Service Provider Association on your proposed "Lawful Access" document.

If you have any questions regarding our letter, please feel free to call me at 202 778 3576.

Thank you for the opportunity to comment on your proposal.

Regards,

[REDACTED]  
ISPA

[REDACTED]  
Washington, DC  
[REDACTED]



US Internet Service Provider Association

1330 Connecticut Avenue, N.W. ♦ Washington, DC 20036 ♦ 202.862.3816 (v) ♦ 202.261.0604 (f)

December 13, 2002

The Honorable Martin Cauchon, P.C. M.P.  
Minister of Justice and Attorney General  
Department of Justice Canada  
284 Wellington Street  
Ottawa, Ontario K1A 0N2  
Canada

Dear Minister Cauchon:

I'm writing on behalf of the US Internet Service Provider Association (US ISPA), a trade association representing large Internet Service Providers (ISPs), many of which serve customers in Canada. Our members include America Online, Tele globe, Cable & Wireless, EarthLink, eBay, SBC Communications, Verizon, and WorldCom. We write to request that a more detailed version of the Department of Justice's proposed "Lawful Access – Consultation Document" be made available to interested parties. Without the draft legislation and accompanying regulation, US ISPA is not able to provide you with detailed comments on the possible financial and operational effects the proposed legislation may have on the industry.

Last month, the Department of Justice met with some of our member companies and the Canadian ISP industry to unveil and discuss new surveillance proposals outlined in "Lawful Access – Consultation Document." We very much appreciate this effort to reach out to the ISP industry and to establish an open dialogue on the ideas in your consultation paper. Unfortunately, the broad concepts in the "Lawful Access" document do not provide enough details on the specific language and breadth of the regulation to allow us to develop a constructive and comprehensive response. The paper does, however, raise significant questions on how standards will be developed, how the law will be implemented, who will pay for the implementation, and whether or not certain agenda items are technically feasible. The document also leaves critical concepts too vague and ill-defined to interpret. For instance, it is entirely unclear what constitutes a "significant upgrade" and whether such an upgrade would require an ISP to make its entire network compliant or only those portions which are upgraded.

It is critical that the ISP industry and the Department of Justice work closely together to understand the costs and unintended consequences associated with this proposed legislation. US ISPA fears that some of the proposals may decrease incentives for technological innovation and competitive advantage in Canada. We understand this is not your intent. On the contrary, in

The Honorable Martin Cauchon, P.C. M.P.

December 13, 2002

Page 3

proposal provides a strong disincentive for technological innovation and investment in Canadian ISPs.

For these reasons, we request that the draft legislation and accompanying regulations be made available for a full and complete public review and that sufficient time be provided for interested parties to assess their impact and submit comments.

Respectfully submitted,



s.19(1)

US Internet Service Provider Association

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 16 11:59 AM  
To: la-al@justice.gc.ca  
Subject: Public Consultation on Lawful Access Proposals



L-Dec4-Lawful Access

Submissio...

On behalf of the Canadian Public Policy Committee of the Computing Technology Industry Association (CompTIA) I am pleased to provide the attached submission in response to the public consultation on lawful access to information and communications.  
Yours truly,

[REDACTED]  
TACTIX Government Consulting Inc.  
World Exchange Plaza  
45 O'Connor Street, Suite 880  
Ottawa, Ontario  
K1P 1A4

Tel: (613) 566-7053

mailto: [REDACTED]

web: <http://www.tactix.ca/>



December 16, 2002

Submitted by e-mail to: [la-al@justice.gc.ca](mailto:la-al@justice.gc.ca)

Lawful Access Consultation  
Criminal Law Policy Section  
Department of Justice Canada  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, ON K1A 0H8

**Re: Public Consultation on Lawful Access Proposals**

The Canadian Public Policy Committee of the Computing Technology Industry Association (CompTIA) welcomes the opportunity to participate in the public consultations regarding lawful access to information and communications. It is timely and appropriate for the federal government to assess whether current laws adequately take into account the rapid evolution of technology and the uses, both positive and negative, which can be made of this technology.

**1. Balancing Competing Public Policy Objectives**

The policy issues raised by proposals to provide lawful access to information and communications are critically important. A careful, deliberate balancing of competing policy objectives is absolutely essential. Law enforcement and national security agencies require appropriate tools to investigate serious crimes and threats to national security. At the same time, privacy rights and the rights guaranteed by Canada's *Charter of Rights and Freedoms* must be respected, protected and upheld.

It is not possible, however, to adequately weigh these competing objectives based on the government's August 25, 2002 public consultation document. This document does not contain sufficient information about difficulties faced by law enforcement and national security agencies under current laws to ascertain if additional measures that may compromise privacy and *Charter* rights to some extent are warranted. In the absence of such information, it is difficult to be persuaded that additional powers in the hands of law enforcement and national security agencies are essential.

Although the information available in the public consultation document does not enable us to offer our views as to whether competing policy interests are balanced appropriately, we are able to suggest a key principle to guide the government's approach to lawful access to information and communications. We understand and accept that Canada's legal framework should be updated where necessary to ensure it applies to new

CompTIA Canadian Public Policy Committee  
c/o TACTIX Government Consulting Inc.  
World Exchange Plaza  
45 O'Connor Street, Suite 880, Ottawa, Ontario K1P 1A4  
Tel: (613) 566-7053 E-Mail: 

s.19(1)

technologies. As a guiding principle, however, the ability to intercept and monitor relatively new forms of communication such as wireless and Internet communications should be based on the same terms and conditions as is the case today for traditional mail and telephone communications, including the same form of judicial authorization and standard of proof.

The consultation document makes it clear that one of the reasons for the proposals to amend the *Criminal Code* to provide for, among other things, production orders and preservation orders, is to enable Canada to ratify the Council of Europe *Convention on Cyber-Crime*. While international cooperation is increasingly essential to investigations of crimes and national security threats, it bears noting that the *Convention* itself contains safeguards that must be respected by signatories. For example, Article 15 of the *Convention* provides that:

- Parties must ensure that the powers and procedures provided for in the *Convention*, including production orders and preservation orders, are subject to conditions and safeguards provided for under their domestic laws, which shall provide for adequate protection of human rights and liberties.
- Conditions and safeguards must include judicial or other independent supervision, grounds justifying application, and limitation of the scope and duration of any power or procedure.

It is clearly the responsibility of the parties to the *Convention* to ensure that the steps they take to bring themselves into compliance with its terms protect human rights and liberties and are in accordance with their domestic legal framework. Thus, should Canada decide to ratify the *Convention*, it can do so while adhering to our country's core legal values and principles.

## 2. Compliance Costs

In addition to ensuring that any new investigatory powers are balanced appropriately against privacy and *Charter* rights, it will also be important for policy makers to take into account any significant compliance costs that may arise as a result of changes to the lawful access process. For example, the public consultation document proposes that all service providers – wireless, wireline and Internet – be required to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies. At a minimum, a “basic intercept capability” would be required before providing new services or a significantly upgraded service to the public. The consultation document does not make clear, however, what constitutes a basic intercept capability nor does it indicate how any significant costs that may be associated with meeting such a standard would be absorbed.

Moreover, it should be noted that, although Articles 20 and 21 of the Council of Europe *Convention on Cyber-Crime* require parties to adopt measures compelling a service provider to collect or record, and to cooperate and assist authorities to collect or record,

traffic data in real time, a service provider is to be so compelled "within its existing technical capability". It will be interesting to learn how this provision of the *Convention* would be reconciled in Canada's approach to basic intercept capabilities.

### 3. CompTIA's Canadian Public Policy Committee

CompTIA's Canadian Public Policy Committee represents the public policy interests of the 600 Canadian members of the Computing Technology Industry Association, a global not-for-profit trade association for the information and communications technology industry. Founded in 1982, CompTIA represents more than 13,000 members in 89 countries. Almost 750,000 individuals worldwide have earned one or more of CompTIA's vendor-neutral certifications that assess technology skills.

The greatest strength of CompTIA lays in its representation of the full spectrum of the computing and communications industry across Canada. Our members range from multinational computer hardware, software and semiconductor manufacturers to small businesses specializing in the service and repair of computer and communications equipment. CompTIA membership also includes solutions providers, computer distributors, in-store retailers, online retailers, training organizations and Internet companies.

We trust that this submission assists the Departments of Justice, Industry Canada and the Solicitor General of Canada in their deliberations on the question of lawful access to information and communications.

Yours truly,

s.19(1)

Chair, CompTIA Canadian Public Policy Committee,  
President, CompuSmart Edmonton



Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 16 11:52 PM  
To: la-al@justice.gc.ca  
Subject: Lawful Access or Lazy Access?

s.19(1)

Lawful Access or Lazy Access?

[REDACTED]  
Ottawa ON  
[REDACTED]

#### I. DEFINITIONS

Target - person or organisation subject to a communications interception order.

Subscriber - person or organisation with a continuing, identified, relationship with a Service Provider.

Box - any electronic device

#### II. INITIAL PROBLEMS

There are many types of Service Providers extant. Many, including universities, libraries, Internet caf,s, and others do not require subscription, preventing Targeted lawful access without infringing the privacy of tens, hundreds, or thousands of other people

#### III. REQUIREMENT TO ENSURE INTERCEPT CAPABILITY

There are many problems with this.

1) Internet communications are bundled into one or more communications streams from the Service Provider to the rest of the Internet. Allowing police access to one or more streams would infringe on the privacy of

thousands or tens of thousands of other clients of the Service Provider

2) Individual communications are broken into many packets within a communications stream. These may proceed by many dynamically changing paths between source and destination. These packets themselves

may be aggregated into larger chunks or split into smaller chunks (e.g. Asynchronous Transfer Mode) -

dynamically. Any Targeting of a particular Subscriber by a single Box is next to impossible.

3) Targeted Subscribers to a Service Provider might connect via any of the Subscriber access ports. It is common for there to be no single place or address that their transmissions pass through all the time.

4) Email addresses are easier, quicker, and cheaper to create and discard than personal AKAs. There is no necessary connection to any particular Subscriber. Subscriptions are almost as easily multiplied.

5) Email addresses may be easily created on mail servers in different countries on different continents and accessed from anywhere.

6) Strong encryption, which has many commercial and practical uses, will largely prevent understanding conveyed illegal messages, especially if they are distributed along multiple paths.

7) For web access or email, Targets can have multiple accounts with different Service Providers or use

Internet access that does not identify who is using it, e.g. an Internet caf,.

1), 2), and 3) imply that the only way to intercept the communications of a particular Subscriber is for the

Service Provider to actually do all the work of picking out their communications. No attached magic Box will do

it without horrendous expense and Service Provider parameters, and any such magic Box would inevitably

infringe the privacy of thousands of non-Targets.  
Since Service Providers use their own mix of hardware and software, no single computer program would achieve the surveillance required. A whole variety of such programs would have to be written and updated as other software and hardware is updated. Installation would be problematical and it is likely to form a substantial workload for the Service Provider to install.  
Such a program, installed by the Service Provider would also provide Service Provider technicians with an easy way to infringe any Subscriber's privacy. The technicians are not police, with police training and discipline.  
This policy would also make each Service Provider a police officer or spy, without pay or police administration.  
This would be a foolish and dangerous policy.  
Is this Lawful Access or Lazy Access  
4), 5), 6), and 7) imply that a Target can easily, quickly, and cheaply escape surveillance. Causing all Service Providers to install special software and extra hardware to handle surveillance efforts is a foolish expense that will raise costs substantially for all Subscribers, or for the government if it will be covering Service Provider costs.

#### IV. FORBEARANCE

Why not just delay the signing of the bill?

#### V. COMPLIANCE

This can be handled by the courts in regards to particular court orders.

#### VI. COSTS OF ENSURING INTERCEPT CAPABILITY

If this is ever implemented, it would be a substantial burden to all Service Providers. All initial costs should be born by the government.  
Costs to update the capability when other parts of the Service Provider system change should be born by the government.

Costs should include hardware, software, and Service Provider labour and expenses.

#### VII. GENERAL PRODUCTION ORDERS

Production orders that are not subject to the same safeguards as Search warrants would be an unjustifiable abomination to the Charter of Rights and Freedoms.

The proper way to access data is to get a Search or Interception order.

#### A. Extraterritoriality

The paper also states, "Such production orders could also allow law enforcement officials to obtain documents in cases where a search warrant cannot be delivered because the documents are stored in a foreign country."

How would this extraterritoriality work? Would Canada consent to other countries enforcing order on our soil?

This is madness.

#### VIII. SPECIFIC PRODUCTION ORDERS

#### A. "Traffic data"

Why should the public have a lower expectation of privacy for the telephone numbers they call or the Internet

addresses they access. Would you want the public to know you called a sex-talk line or accessed

<http://www.barely-legal-babes-to-fuck.com> or <http://www.I-Love-Hitler?> or [http://I-Love-To-Be-](http://I-Love-To-Be-Dominated.com)

[Dominated.com](http://I-Love-To-Be-Dominated.com) Surely the addresses you go to or the numbers you call should be a private matter without

reasonable grounds to suspect an offence has or will be committed.

Much Internet access is done from the home, even the bedroom. Why should police be entitled to snoop on these without reasonable grounds.

The proper way to access traffic data is to get an Interception warrant.

#### IX. ORDERS TO OBTAIN SUBSCRIBER AND/OR

#### SERVICE PROVIDER INFORMATION

Are web sites to be considered Service Providers? Especially if they have chat rooms or an email list service?

Since most web sites have a particular focus, e.g. gay sex, revealing who their Subscribers are would disclose the lifestyle preferences of their Subscribers. The same may be true of other types of Service Providers.

What if the Subscriber indicates when they subscribe that they want their information to be private as a

condition of service? Many subscription forms ask explicit permission to reveal Subscriber information to others

and the Subscriber can, and often does, deny it. What then is the Subscriber's expectation of privacy?

If the Service Provider does not collect any sought-after information on its clients, then the police should not be allowed to impose that on them. Many Service Providers are greatly automated and changing the system to

accommodate particular requests is not cheap, and it would also be a burden and possibly an invasion of

privacy for all the existing clients.

The proper way to access data is to get a Search warrant.

#### X. ASSISTANCE ORDERS

Orders that facilitate police access should be acceptable, but orders that require programming or system

administration effort should be paid for by the police at commercial rates.

#### XI. DATA-PRESERVATION ORDERS

A reasonable period is four days without a Search or Interception Warrant.

It is unclear what this would apply to. All data communication lives in various buffers on its way to or from a

client, sometimes for several seconds. Data Preservation orders should only apply to records ordinarily created

and stored for at least a day in the ordinary course of business. This would allow Service Providers to make

extra backups when needed.

#### XII. VIRUS DISSEMINATION

"Further, in order to ratify the Convention, new offences in relation to illegal devices (such as viruses) would

have to be added. These could include importation, procurement for use, and otherwise making available an

illegal device as defined in the Convention."

Without the intent to commit an offence, these should be legal. How are virus-fighters to analyse viruses? How

are researchers to analyse the growth and changes in viruses, encryption, and other devices so as to better

understand them?

I also worry that this provision would cover "devices" which are not viruses and are intended for legal private

copying and backup of copyrighted materials and playing of DVD movies from other regions.

#### XIII. INTERCEPTION OF E-MAIL

If the eMail is at the Addressee's facilities, a Search or Interception and Seizure order should be sufficient.

If the eMail is at the Service Provider's facilities (or intermediate 3rd party's), an Interception order should be made.

This will simplify administration and preserve the privacy of our communications. If we wish received emails (or

letters) to remain private, we can always destroy them after reception.

#### XIV. OTHER MECHANISMS TO PROVIDE SUBSCRIBER AND SERVICE PROVIDER

##### INFORMATION

Compelling Service Providers to collect CNA information is very foolish in the case of mobile phones, email

addresses, or Internet access.

Do you expect libraries and Internet cafés to require current government identification with addresses and to

record these every time a client seeks access? What about children at the library? What is the advantage gained

by these actions by millions of people when they are so easily bypassed?

Prepaid cellular telephones are easily sold or given away, rendering the official CNA useless.

# XV. CONCLUSION

The government should not expect that intercepting Internet access is easy and inexpensive. There are no international spying standards, especially ones which respect the privacy rights of citizens.

It would be wiser to move slowly in this area and retain the good will of Service Providers and citizens.

Interception of e-mail

---- Quidquid latine dictum sit altum videtur ----

①  
- \ <  
(\*) / (\*)

Ottawa ON Canada

s.19(1)

"They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." -- Benjamin Franklin

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 16 11:59 PM  
To: Department of Justice Canada  
Cc: Mr. John Godfrey, MP  
Subject: Lawful Access s.19(1)

Dear Sirs:

I have read the Lawful Access Consultation Document in its entirety at <[http://canada.justice.gc.ca/en/cons/la\\_al/index.html](http://canada.justice.gc.ca/en/cons/la_al/index.html)> and am distressed over attempts by the government to pass laws that I believe blatantly violate the Charter and civil rights of Canadians. I only found out about the deadline a few days ago so I cannot go into as much detail as I would like about all the things that I find odious about these proposals. A few that come to mind immediately are:

1. There is an underlying assumption that criminals and terrorists, ostensibly the reason why this legislation is necessary to enact, do not already use strong cryptography. This is a flawed assumption at best and dishonest at worst. I suspect this fact is known to you already but that you have some even more odious legislation up your sleeves after the passage of legislation based upon these proposals, such as forced disclosure of private keys or key escrows.
2. There is an underlying assumption that there are choke points whereby one could have the technical means to intercept electronic communications. It is not entirely obvious that such choke points exist since the Internet is a web of networks. It was designed to be distributed and self-healing and as such, can easily circumvent defects, such as attempts at controls by repressive governments.
3. Data preservation orders would be impractical and discriminate against smaller ISPs. This would further consolidate the market position of the telecom and cable television oligopolies in the ISP business. Unless the government is willing to come up with fantastic sums of money to fund the technology necessary to do these things, it would be impossible for ISPs to implement the proposed changes on their own. I would object to such frivolous expenditures by government. If ISPs were expected to fund these measures, it would seriously damage the competitiveness of the Canadian ISP industry and hurt consumers.

My objections are not limited to those above. Virtually every proposal put forth is unacceptable and offensive in the extreme. Suffice to say that a government that passed the Firearms Act, an act which violates the Charter, civil, and privacy rights of firearms owners using lies and junk science as a justification for that legislation, and subsequently spent 500 times the initially projected amount to prop up said legislation, has little credibility with me. It would appear that this government is completely brazen and shameless in its pursuit of exercising unconstitutional and unlawful power over its citizens. It further appears that this government pushes the boundaries as far as possible knowing that ordinary citizens, like me, do not have the resources or the time to mount legal challenges to every unconstitutional and illegal law that is passed. It should not be this way. Canadians deserve better. The Liberal Party seems to have lost its way and will pay at the ballot box at the next election as a result.

Yours truly,

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Dec 16 12:23 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Document d'Option consommateurs

s.19(1)



Interception.doc

Bonjour

Voici la version électronique du document d'Option consommateurs sur  
l'interception des communications électroniques au Canada.

Bonne journée

[REDACTED]  
Option consommateurs

**Chimères et surveillance:  
l'interception des  
télécommunications et la  
vie privée au Canada**

**observations présentées au  
ministères de la Justice, de  
l'Industrie et du Solliciteur général  
du Canada par**

**Option consommateurs**

**16 décembre 2002**



La surveillance électronique est à ce point efficace qu'elle rend possible, en l'absence de toute réglementation, l'anéantissement de tout espoir que nos communications restent privées. Une société nous exposant, au gré de l'État, au risque qu'un enregistrement électronique permanent soit fait de nos propos chaque fois que nous ouvrons la bouche, disposerait peut-être d'excellents moyens de combattre le crime, mais serait une société où la notion de vie privée serait vide de sens.

*R. c. Duarte*, [1990] 1 R.C.S. 30

## Sommaire

Le ministère de la Justice, le ministère de l'Industrie et le Solliciteur général du Canada procèdent à une consultation relative à l'extension des pouvoirs de surveillance des services policiers et des autorités chargées de la protection de la sécurité nationale dans le domaine des télécommunications. Ils formulent une série de propositions, qu'il faut interpréter dans le contexte de la signature par le Canada de la Convention sur la cybercriminalité du Conseil de l'Europe et à la lumière des règles du droit constitutionnel canadien. Dans ce contexte, nous émettons l'avis que les justifications avancées à l'égard des propositions ministérielles demeurent tout à fait insuffisantes et inadéquates, que l'implantation de certaines de ces propositions pourrait menacer sérieusement la protection des droits fondamentaux des Canadiens et que ces propositions devraient donc pour la plupart être écartées.

Le document de consultation diffusé par le gouvernement du Canada ne fournit en effet pratiquement aucune donnée visant à expliquer les problèmes auxquels feraient présentement face les autorités chargées de la police et de la sécurité nationale. On s'en tient à quelques énoncés très généraux, dont certains ne résistent d'ailleurs pas à une analyse sommaire. Le fardeau de convaincre la population que des réformes sont requises repose en l'instance sur l'État, qui ne s'en est pas déchargé. Il en résulte que le document de consultation élude les questions fondamentales, liées au «pourquoi», pour se concentrer sur des questions de détail liées au «comment». Or on ne peut faire l'économie de l'analyse des besoins et des objectifs poursuivis, ne serait-ce que pour pouvoir à l'avenir déterminer si ces objectifs ont été atteints.

D'autre part, les tribunaux canadiens ont établi des critères élevés en matière de contrôle des activités de surveillance électronique de l'État. Certaines des propositions formulées pourraient ne pas s'y conformer entièrement, notamment en ce qu'elles auraient pour effet d'institutionnaliser des mesures de surveillance et de porter systématiquement atteinte à la liberté d'expression.

Plus précisément, le document de consultation évoque d'abord l'hypothèse d'imposer à tous les fournisseurs de service de télécommunication l'obligation de configurer leurs systèmes de telle manière que les autorités puissent en tout temps procéder à l'interception des données transmises. L'implantation d'une telle mesure serait fort coûteuse, et pourrait bien être vaine parce que les criminels et les terroristes les plus avertis pourraient en contourner les effets, à moins qu'on établisse un régime de censure des communications indéchiffrables. Elle aurait des effets délétères graves sur la protection de la vie privée et la liberté d'expression. Elle nuirait aussi significativement au progrès technologique dans ce domaine, et donc au développement d'un pan important de la structure industrielle canadienne. Cette proposition devrait donc être écartée d'emblée.

Le document décrit ensuite divers types d'ordonnances de production qui pourraient être ajoutés à l'éventail de telles ordonnances existant déjà en droit canadien. On s'inquiète d'abord de la prolifération d'outils procéduraux, qui ne concourt pas à la simplification du droit. On s'inquiète ensuite de la volonté affichée que certaines de ces ordonnances puissent être obtenues même dans des circonstances où un magistrat n'a pas été convaincu qu'il existe des motifs raisonnables de croire qu'une infraction a été commise ou le sera vraisemblablement. L'analyse présentée dans le document de consultation sous-estime à maints égards la sensibilité de divers types de renseignements, dont les données de trafic relatives aux télécommunications. Il y aurait lieu de simplifier et d'harmoniser ces diverses propositions, et de ne pas permettre l'émission des ordonnances envisagées sans qu'un juge d'une cour supérieure ait été convaincu de la commission ou de l'imminence d'une infraction.

On envisage également d'établir en droit canadien des ordonnances d'obtention de données qui imposeraient un fardeau important à leurs destinataires, dont la portée n'est pas bien délimitée et qui pourraient avoir un effet extraterritorial antithétique aux pratiques traditionnelles du Canada en cette matière. Là encore, la nécessité qu'un tel instrument soit créé n'est pas démontrée et la proposition gouvernementale comporte peu d'éléments qui permettent de l'évaluer précisément.

En somme, la preuve et les arguments soumis par le gouvernement dans le document de consultation ne convaincraient vraisemblablement pas un tribunal du bien-fondé des propositions y formulées ou de leur conformité au droit constitutionnel. On ne voit pas que l'opinion publique pourrait, sur la foi des mêmes éléments, donner son aval à ces propositions.

Il faut enfin noter que plusieurs d'entre elles sont liées à l'adaptation du droit canadien aux obligations qui découleraient de l'éventuelle ratification par le Canada de la Convention sur la cybercriminalité. Cette ratification imposerait aussi d'autres obligations au Canada en matière de coopération internationale. Pour ces motifs, il nous paraît qu'il serait à tout le moins prématuré que le Canada ratifie cette Convention.

Les questions soulevées dans cette consultation, dont il est heureux qu'elle soit tenue, sont de la plus haute importance pour le respect des droits fondamentaux au Canada et le développement des modes de télécommunication. Le débat qui les entoure doit donc se poursuivre, mais il doit être éclairé par la présentation de la part du gouvernement du Canada des éléments qui permettraient d'en mieux comprendre tous les enjeux.

## Table des matières

I- Introduction.....	1
A- Le contexte .....	1
B- La présentation.....	3
1- l'intervenante.....	3
2- le plan .....	3
II- L'analyse des mesures proposées .....	4
A- L'urgence, l'ombre, Thémis.....	4
1- l'ampleur des besoins .....	4
2- le cadre constitutionnel .....	6
a) le partage des compétences .....	6
b) la Charte canadienne .....	7
i) les règles substantives .....	7
ii) l'évaluation selon l'art. premier .....	14
B- Les propositions étatiques.....	16
1- les modifications technologiques.....	16
2- les ordonnances générales de production.....	27
3- les ordonnances spécifiques de production.....	33
4- les ordonnances d'obtention de données .....	37
5- les ordonnances d'assistance .....	38
6- les ordonnances de conservation .....	41
7- la propagation des virus .....	44
8- l'interception du courriel .....	44
9- les modifications à la Loi sur la concurrence .....	47
10- d'autres modifications législatives.....	48

## **Notes et remerciements**

L'auteur de ces observations a bénéficié au cours des douze dernières années de la collaboration d'un grand nombre de personnes qui s'intéressent activement au domaine de la protection de la vie privée et des renseignements personnels. Il les remercie tant de leur éclairage au fil des ans que des débats auxquels ils ont bien voulu participer.

À l'égard des questions soulevées dans cette étude, on soulignera notamment les apports en 2001 et au début de 2002 de Mme Stephanie Perrin et de M. Ian Hosein.

L'auteur tient également à remercier Option consommateurs pour de multiples raisons, y compris l'occasion qu'elle lui a donné de se pencher sur les questions relatives à la protection des renseignements personnels depuis une douzaine d'années.

La reproduction d'extraits limités du texte de ce rapport est permise, à condition qu'en soit mentionnée la source. Sa reproduction à des fins publicitaires ou lucratives est toutefois strictement interdite, tout comme l'est toute allusion à son contenu à de telles fins.

### **Dépôt légal**

Bibliothèque nationale du Québec  
Bibliothèque nationale du Canada

ISBN 2-921588-45-5

Option consommateurs

2120, rue Sherbrooke est, bur. 604

Montréal, Qc

H2K 1C3

téléphone: (514) 598-7288

télécopieur: (514) 598-8511

adresse électronique: [courriel@option-consommateurs.org](mailto:courriel@option-consommateurs.org)

# Chimères et surveillance: l'interception des télécommunications et la vie privée au Canada

## I- Introduction

### A- Le contexte

Le ministère de la Justice, le Solliciteur général et le ministère de l'Industrie du Canada procèdent présentement à une consultation relative à la modification de diverses dispositions législatives relatives à l'interception et à l'obtention de communications transmises par voie électronique par les corps policiers et les organismes chargés de la protection de la sécurité nationale au Canada. Les modifications envisagées visent notamment à permettre à ces corps policiers et organismes d'adapter leurs capacités de cueillette d'informations aux nouvelles technologies, dont l'Internet. Elles auraient un impact sur le *Code criminel*, la *Loi sur la concurrence* et, potentiellement, d'autres lois canadiennes<sup>1</sup>. Il faut d'autre part les analyser dans le contexte de la signature par le Canada de la Convention sur la cybercriminalité, le 23 novembre 2001<sup>2</sup>.

Les orientations gouvernementales dans ce domaine se clarifient à la lumière de cette consultation, et il faut s'en réjouir. On ne peut évidemment que souscrire en principe à la volonté que les activités criminelles ou terroristes soient réprimées, et que les entités à qui ces missions sont confiées soient dotées des outils qui leur permettent de les accomplir. La fin ne justifie cependant pas tous les moyens, et la lutte contre le crime et le terrorisme ne constitue pas le seul objectif de politique publique devant guider l'action du Parlement et du gouvernement canadiens. La préservation de l'ensemble des droits fondamentaux de tous les Canadiens doit demeurer l'une des assises essentielles de cette action.

---

<sup>1</sup> Quant à la description des modifications envisagées, Justice Canada; Industrie Canada; Solliciteur général du Canada. *Accès légal – Document de consultation*. Ottawa, gouvernement du Canada, 25 août 2002. 25 p. (ci-après le «Document de consultation»).

<sup>2</sup> On trouvera des renseignements à l'égard de la Convention ainsi qu'un lien vers son texte au <http://conventions.coe.int/Treaty/FR/CadreListeTraites.htm>. En vertu de ses dispositions, elle entre en vigueur sur ratification de 5 signataires, dont 3 États membres du Conseil; jusqu'à maintenant, seules l'Albanie et la Croatie auraient ratifié la Convention.

Or, même si beaucoup d'éléments demeurent méconnus, on peut au moins esquisser une évaluation de la teneur des propositions contenues dans le Document de consultation et de certaines des conséquences que pourrait avoir leur mise en oeuvre sur les citoyens, et cette première évaluation incite à croire qu'on est en voie de déséquilibrer davantage les relations entre l'État et les citoyens, sans que la démonstration ait été faite de manière convaincante que cette opération s'imposait.

À première vue, en effet, on ne voit pas d'élément qui permette à l'observateur impartial de prendre précisément la mesure du péril que constitueraient les nouvelles technologies de communication pour le maintien de l'ordre public. On ne voit pas non plus très bien où se situent les limites du nouveau champ d'intervention que veulent patrouiller nos policiers, et certaines indications dans le Document de consultation donnent à penser que les autorités sous-estiment considérablement l'impact qu'auraient les pouvoirs dont on voudrait les doter sur le respect des droits fondamentaux, et notamment du droit à la vie privée.

On se rangera donc ici dans le camp des observateurs perplexes, sinon inquiets. Trop de données manquent encore pour bien jauger les effets qu'aurait l'implantation des mesures envisagées et celles qu'il fournit ne suffisent pas à rassurer. Compte tenu de la gravité des enjeux, la précipitation serait à notre avis bien mauvaise conseillère.

On sait que ces questions font l'objet de discussions à l'échelle internationale. On sait que ces débats se mènent dans bien des cas en vase clos, les citoyens se trouvant pratiquement mis devant le fait accompli parce que des représentants de la Couronne ont donné à nos partenaires internationaux des indications quant aux orientations vraisemblables de la législation canadienne. On sait très bien le contexte international actuel, et la vigueur des recommandations que nous font certains partenaires étrangers quant aux politiques canadiennes en matière de sécurité nationale. On sait que la technologie progresse, et que les citoyens l'utilisent de plus en plus sans pour autant comprendre comment elle fonctionne, et à quels abus elle peut donner lieu. On en conclut que sagesse et précipitation ne vont pas de pair.

On sait aussi, et on le verra plus précisément *infra*, que les effets des propositions gouvernementales toucheraient tous les citoyens, et pas seulement les criminels dangereux ou les terroristes. On s'en inquiète. Et on peut même craindre légitimement qu'au bout du compte, les honnêtes citoyens feraient davantage les frais de cette extension des pouvoirs

policiers que les criminels ou les terroristes. La véritable démocratie requiert que l'État de droit n'ait pas tous les droits.

Il est à cet égard heureux que le gouvernement du Canada ait entamé un processus de consultation et qu'il y ait inclu les représentants de la société civile, à l'occasion notamment de trois (3) rencontres tenues au cours de l'automne 2002 à Ottawa, Montréal<sup>3</sup> et Vancouver. Ce processus doit se poursuivre et s'amplifier, afin que les citoyens puissent porter un jugement éclairé à l'égard de ces questions.

Les quelques pages qui suivent nous donnent l'occasion de formuler certains commentaires à l'égard des propositions gouvernementales, que nous serions toutefois tentés de qualifier de «préliminaires», compte tenu notamment des éléments mentionnés dans la section II-A. L'absence de commentaire dans ces pages à l'égard de l'une ou l'autre des questions abordées dans le Document de consultation n'indique ni un accord, ni un désaccord avec les propositions gouvernementales.

## B- La présentation

### 1- L'intervenante

Option consommateurs<sup>4</sup> a été constituée en personne morale en 1983. Elle a succédé dans sa région à l'Association coopérative d'économie familiale de Montréal, qui existait depuis 1967. Il s'agit d'un organisme coopératif de défense et de promotion des droits des consommateurs qui n'est affilié à aucun autre mouvement. Elle intervient dans de nombreux domaines et compte présentement une équipe de vingt-deux (22) personnes.

Option consommateurs s'intéresse activement depuis 1990 aux questions relatives à la protection des renseignements personnels. Elle a notamment comparu à diverses reprises en commission parlementaire (à Québec et à Ottawa) ou auprès d'autres instances afin de commenter divers projets de loi ayant trait à ces questions, à leur impact dans le domaine des télécommunications ou à l'implantation d'une carte d'identité. Elle a également participé à de nombreuses instances auprès du Conseil de la radiodiffusion et des télécommunications canadiennes (ci-après également le «CRTC») qui avaient trait à ces questions.

---

<sup>3</sup> Option consommateurs a contribué activement à l'organisation de la rencontre de Montréal.

<sup>4</sup> «Option consommateurs» constitue depuis le mois de septembre 1997 la raison sociale de l'Association coopérative d'économie familiale du Centre de Montréal, ou «ACEF-Centre».



## 2- le plan

On formulera dans les quelques pages qui suivent des commentaires relatifs aux principales questions soulevées dans le Document de consultation, et on suivra l'ordre des problématiques qui y sont abordées. On formulera cependant d'abord une critique d'ensemble de la teneur du Document en mettant l'accent sur ce qu'il ne contient pas, avant d'esquisser les contours de certaines au moins des règles de droit constitutionnel pertinentes dans ce débat.

En somme, le Document joue fort efficacement un rôle provocateur. Il expose les lacunes qui subsistent dans la rhétorique gouvernementale. Et il démontre à l'envi qu'il importe de discuter vigoureusement de ces questions, afin qu'une ne soit pas implanté dans notre société un régime qui ferait peu pour améliorer la sécurité collective et qui serait attentatoire aux droits.

### **Première recommandation**

**Nous recommandons que les propositions contenues dans le Document de consultation fassent l'objet d'une vaste consultation publique, soutenue par la publication de toutes les informations qui y sont nécessaires et portant sur l'ensemble de la problématique, et qu'aucune de ces propositions ne soit mise en oeuvre avant que cette consultation soit terminée.**

## **II- L'analyse des mesures proposées**

### **A- L'urgence, l'ombre, Thémis**

#### **1- l'ampleur des besoins**

Il s'agit de modifier la législation canadienne afin d'accorder aux autorités policières et aux organismes chargés de la protection de la sécurité nationale des pouvoirs plus étendus ou plus précis en matière d'interception ou d'obtention du contenu de communications transitant par voie électronique ou d'autres éléments liés à ces communications. Pour les raisons auxquelles on reviendra à la section suivante, cela met en cause la protection des droits fondamentaux, garantis aux citoyens par la constitution canadienne. On s'attendrait donc qu'une démonstration convaincante soit faite de l'ampleur des problèmes éprouvés par les autorités et de l'urgence qu'il y aurait à agir.

Or cette démonstration n'est nulle part faite, ni même esquissée, et surtout pas dans le Document de consultation. Certes, on trouve<sup>5</sup> quelques affirmations générales: de nouvelles technologies émergent, elles sont utilisées par les criminels, l'«accès légal»<sup>6</sup> importe aux forces de l'ordre... Cela ne suffit pas à alimenter un débat public, ni à justifier des mesures législatives attentatoires aux droits fondamentaux.

Dans combien de cas les autorités canadiennes ont-elles été empêchées de mener une enquête ou de procéder à une arrestation dans les deux dernières années parce qu'elles ne disposaient pas de pouvoirs tels que ceux dont on recommande la mise en place? Quelles étaient les nouvelles technologies utilisées, et quelle était exactement la difficulté qui a empêché les autorités d'agir? On l'ignore absolument. Faute de mesurer le problème, on ne peut se prononcer précisément sur l'adéquation des solutions proposées. On ne sait pas davantage si on retrouvait dans ces cas une dimension transfrontalière, qui ajoute une dimension singulièrement importante à la problématique, surtout dans le contexte de l'éventuelle ratification de la Convention sur la cybercriminalité.

D'autre part, quelle évaluation peut-on faire des mesures législatives déjà en place? Le régime actuel des interceptions de communications téléphoniques, par exemple, établi en 1974, fonctionne-t-il adéquatement à l'égard des activités qu'il vise? Les intérêts de l'État et ceux des prévenus y sont-ils bien protégés? Convient-il, par conséquent, de s'inspirer d'un tel régime, ou au contraire de tout remettre sur le métier? On l'ignore également. On se condamne donc à légiférer à la pièce, en risquant de multiplier les outils procéduraux permettant l'interception d'information, avec les avantages que cela comporte pour les corps policiers qui voudront choisir dans chaque cas l'instrument qui leur convient le mieux, et les inconvénients que comporte pour toutes les parties la multiplication des processus et les risques de confusion et de cafouillage.

En troisième lieu, comment évolue la conjoncture criminelle et terroriste? Quelle vision d'ensemble en a-t-on, et de quel plan d'action global se dote-t-on? Comment évolue la répartition des responsabilités entre les divers corps policiers et les agences chargés de la sécurité nationale au Canada? Tous ont-ils besoin de tous les pouvoirs dont on envisage la mise en place? À l'égard de quels types de comportements criminels les vastes pouvoirs d'enquête devraient-ils pouvoir être exercés? On ne nous en dit rien.

---

<sup>5</sup> aux pages 3 à 5 notamment.

<sup>6</sup> et notons que cette expression paraît fort imprécise et bien peu élégante, surtout en français. On tentera donc de l'éviter dans toute la mesure du possible dans les prochaines pages.

Bref, le Document de consultation élude soigneusement les questions fondamentales. Il ignore le «pourquoi» pour tenter d'alimenter les discussions de détail à l'égard du «comment». Il s'agit là d'une faille fatale. Elle prive les propositions gouvernementales d'une grande part de la crédibilité qui inciterait à les envisager plus favorablement.

On veut bien admettre que certaines données précises ne puissent pas faire l'objet de débats publics, pour ne pas compromettre des enquêtes ou des méthodes d'enquête notamment. Mais il ne saurait suffire à l'égard de questions de cette importance que les autorités disent aux citoyens: «Faites-nous confiance, il y a péril en la demeure! Si vous saviez ce que nous savons!» D'autant que ce sont les mêmes autorités qui, directement ou indirectement, bénéficieraient de l'extension des pouvoirs dont elles réclament instamment l'établissement.

Et si on en sait bien peu quant à l'ampleur que prendraient les lacunes des moyens policiers, on n'en sait guère davantage à l'égard des modalités des solutions proposées. Nous y reviendrons *infra*; notons simplement que le Document de consultation se fait peu loquace en ce qui a trait aux coûts associés à la mise en place des recommandations formulées ou à leur impact sur les tarifs payés par les clients, ou en ce qui a trait aux détails techniques des mécanismes d'interception du courriel qui pourraient être mis en place, par exemple.

En somme, il s'avère pratiquement impossible de mener un débat de qualité, faute d'informations. On ne peut évaluer dans quelle mesure les propositions gouvernementales permettraient effectivement d'atteindre des objectifs qui ne sont eux-mêmes pas formulés clairement. On devra donc se borner dans les pages qui suivent à la critique des caractéristiques intrinsèques de ces propositions, sans pouvoir émettre d'avis sur leur efficacité potentielle. Faute de faits, on examinera principalement le droit. On dispose au moins à cet égard d'un certain nombre de jalons qui nous sont fournis par la Constitution canadienne et l'interprétation qu'en ont faite les tribunaux, et notamment la Cour suprême du Canada.

## 2- le cadre constitutionnel

### a) le partage des compétences

Avant d'aller plus loin, il importe de rappeler les grandes articulations du cadre constitutionnel canadien en matière d'action policière à l'égard des communications et de

protection des droits fondamentaux. Rappelons d'abord les grandes lignes du partage des compétences, avant de dire un mot des droits fondamentaux.

En vertu de l'alinéa 91 (27) de la *Loi constitutionnelle de 1867*, le droit criminel, y compris la procédure criminelle, relève de la compétence exclusive du Parlement fédéral. L'administration de la justice dans les territoires des provinces relève cependant de leur compétence exclusive, en vertu de l'alinéa 92 (14) de la *Loi constitutionnelle de 1867*. Les questions de défense ressortissent par ailleurs exclusivement au Parlement, en vertu de l'alinéa 91 (7) du même instrument constitutionnel. La ratification des traités internationaux constitue quant à elle une prérogative de la Couronne, mais les modifications au droit interne que peut requérir la mise en oeuvre d'un traité relèvent de la législature, fédérale ou provinciale, qui a compétence à l'égard de la matière visée<sup>7</sup>.

Il en résulte un enchevêtrement complexe d'institutions. Relèvent par exemple du Parlement la Gendarmerie royale du Canada, le Service canadien de renseignements de sécurité et le Centre de la sécurité des communications, tandis que certaines provinces se sont dotées de corps policiers provinciaux et que d'autres ont délégué un certain nombre de compétences à la Gendarmerie royale. Toutes les provinces ont par ailleurs établi des corps policiers locaux. En règle générale, les poursuites en matière criminelle sont menées par les substituts des procureurs généraux provinciaux, tandis que certaines poursuites pénales peuvent l'être par les substituts du procureur général fédéral<sup>8</sup>. Ne disons rien du droit martial.

La compétence législative du Parlement fédéral dans les matières qui nous intéressent ici paraît certes vaste, mais la mise en oeuvre des pouvoirs qui pourraient être dévolus à diverses autorités ne relève pas entièrement des organismes fédéraux: des organismes provinciaux y jouent aussi un rôle, dont l'action peut également être limitée par des lois provinciales<sup>9</sup>.

#### b) la *Charte canadienne*

##### i) les règles substantives

<sup>7</sup> A.G. (Canada) v. A.G. (Ontario), [1937] A.C. 326 (C.P.) (l'affaire des conventions du travail); Arrow River & Tributaries Slide & Boom Co. v. Pigeon Timber Co., [1932] R.C.S. 495, notamment.

<sup>8</sup> R. c. Hauser, [1979] 1 R.C.S. 984.

<sup>9</sup> comme, au Québec, les articles 4 à 9.1 de la *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, qui protègent notamment le droit à la vie privée et qui s'appliquent entre à l'activité de la Sûreté du Québec et des corps policiers municipaux.

Si la *Loi constitutionnelle de 1867* répartit les attributions législatives entre le niveau fédéral et les provinces, la *Charte canadienne des droits et libertés*<sup>10</sup> limite quant à elle les compétences de tous ces législateurs, qui doivent se conformer à ses dispositions parce qu'elles font partie de la Constitution du Canada<sup>11</sup>, tout comme la Couronne elle-même doit d'ailleurs se conformer à la Constitution<sup>12</sup>.

En l'occurrence, c'est principalement l'article 8 de la *Charte canadienne* qui établit les balises fondamentales à l'égard des pouvoirs de l'État en matière de surveillance:

8. Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

Cette disposition vise notamment la protection sans compromis de la vie privée des personnes<sup>13</sup>. Elle a une portée bien plus que procédurale, comme l'a souligné la Cour suprême:

Il faudrait aussi noter que l'art. 8 ne se contente pas d'interdire les fouilles, les perquisitions et les saisies abusives. [...], il va plus loin et garantit le droit à la protection contre les fouilles, les perquisitions et les saisies abusives.<sup>14</sup>

Il s'agit donc d'une protection substantive, de grande ampleur et justifiée par l'importance qu'a la protection de la vie privée dans la préservation d'une société libre et démocratique:

Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle mériterait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l'ordre public. L'interdiction faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'État démocratique.<sup>15</sup>

<sup>10</sup> *Loi constitutionnelle de 1981, partie I*, constituant l'annexe B à la *Loi sur le Canada* (R.-U.).

<sup>11</sup> *Ibid.*, art. 52.

<sup>12</sup> *Operation Dismantle v. La Reine*, [1985] 1 R.C.S. 441, 455, 459, par exemple.

<sup>13</sup> *Hunter c. Southam*, [1984] 2 R.C.S. 145, 155, 167-168.

<sup>14</sup> *R. c. Dyment*, [1988] 2 R.C.S. 417, 427.

<sup>15</sup> *Ibid.*, 427-428.

La Cour a noté par ailleurs que le droit à la protection de la vie privée inclut des aspects territoriaux ou spatiaux, des aspects liés à l'intégrité de la personne et des éléments liés au contexte informationnel<sup>16</sup>. Il s'agit donc d'un droit de grande portée.

Encore faut-il assurer l'équilibre entre ce droit et les autres intérêts de la société. Il se trouve notamment tempéré par l'attente raisonnable en matière de protection de la vie privée qu'a un individu à l'égard d'un élément donné. La Cour suprême a notamment cherché à déterminer les paramètres visant à réaliser cet équilibre dans une série de décisions relatives à la surveillance électronique policière, dont on peut dégager sommairement quelques éléments.

Premier élément de son analyse, la Cour suprême érige en présomption la règle qu'un acte de surveillance électronique par l'État contrevient à l'article 8 de la *Charte canadienne*:

Je commence par affirmer ce qui me paraît l'évidence même, c'est-à-dire le principe général que la surveillance électronique d'un particulier par un organe de l'État constitue une fouille, une perquisition abusive au sens de l'article 8 de la *Charte*<sup>17</sup>.

Voilà un énoncé d'une remarquable fermeté. La Cour s'en explique:

La réglementation de la surveillance électronique nous protège plutôt contre un risque différent: non plus le risque que quelqu'un répète nos propos, mais le danger bien plus insidieux qu'il y a à permettre que l'État, à son entière discrétion, enregistre et transmette nos propos.

Cette protection s'explique par la conscience du fait que, si l'État était libre de faire, à son entière discrétion, des enregistrements électroniques permanents de nos communications privées, il ne nous resterait rien qui vaille de notre droit de vivre libre de toute surveillance. La surveillance électronique est à ce point efficace qu'elle rend possible, en l'absence de toute réglementation, l'anéantissement de tout espoir que nos communications restent privées. Une société

<sup>16</sup> *Ibid.*, 428.

<sup>17</sup> *R. c. Duarte*, [1990] 1 R.C.S. 30, 42. Notons que 5 juges ont abondé avec les motifs du juge La Forest, le juge en chef en venant aux mêmes conclusions dans l'affaire pour des motifs différents.

nous exposant, au gré de l'État, au risque qu'un enregistrement électronique permanent soit fait de nos propos chaque fois que nous ouvrons la bouche, disposerait peut-être d'excellents moyens de combattre le crime, mais serait une société où la notion de vie privée serait vide de sens<sup>18</sup>.

Par conséquent,

[...] lorsqu'une personne a des motifs raisonnables de croire que ses communications sont privées [...], l'enregistrement électronique clandestin non autorisé de ces communications doit forcément être considéré comme la violation d'une attente raisonnable en matière de respect de la vie privée<sup>19</sup>.

Et l'autorisation dont il s'agit ne saurait être accordée que par un juge d'une cour supérieure, «convaincu que d'autres méthodes d'enquête échoueraient certainement ou vraisemblablement» et qu'il existe des «motifs raisonnables et probables de croire qu'une infraction a été commise ou est en voie de l'être et que l'autorisation sollicitée permettra d'obtenir une preuve de sa perpétration»<sup>20</sup>. La Cour suprême a donc placé la barre fort haut à cet égard.

Encore faut-il établir également comment on mesure l'«expectative raisonnable de vie privée» d'une personne dans une situation donnée. Après avoir souligné dans l'arrêt *Wong* que les principes qui l'avaient guidé dans l'affaire *Duarte* s'appliquaient à l'usage étatique de quelque technologie que ce soit<sup>21</sup>, le juge La Forest a opiné pour la majorité dans cet arrêt qu'il s'agit de déterminer

[...] si, en vertu des normes applicables au respect de la vie privée auxquelles on peut s'attendre dans une société libre et démocratique, les agents de l'État devaient se conformer aux exigences de la *Charte*. Cela suppose que l'on se demande si les personnes dont la vie privée a été violée pourraient légitimement prétendre que, dans les circonstances, il n'aurait pas dû

---

<sup>18</sup> *Ibid.*, 44.

<sup>19</sup> *Ibid.*, 47 (soulignés dans le texte).

<sup>20</sup> *Ibid.*, 45.

<sup>21</sup> *R c. Wong*, [1990] 3 R.C.S. 36, 43-44.

être loisible aux agents de l'État d'agir comme ils l'ont fait sans une autorisation judiciaire préalable<sup>22</sup>.

Et le magistrat, évoquant par ailleurs le risque d'une dérive orwellienne<sup>23</sup>, a noté que, dans l'état du droit au moment des événements concernant M. Wong, il n'existait aucune disposition législative permettant à un juge d'autoriser des pratiques de surveillance vidéo comme celles auxquelles la police de Toronto avait soumis cet individu.

D'abondance, le juge La Forest a souligné que M. Wong avait effectivement une attente raisonnable de vie privée dans les circonstances où il fait l'objet de cette surveillance<sup>24</sup>, et qu'il n'est donc pas sans intérêt de rappeler. On l'accusait en effet d'avoir exploité une maison de jeu «flottante» dans une chambre d'hôtel. La Cour a vigoureusement conclu qu'on peut avoir une attente raisonnable de vie privée même lorsqu'on se trouve avec un groupe de gens plus ou moins inconnus, dans le but de commettre un acte illégal, dans un lieu tel qu'une chambre d'hôtel, ajoutant qu'il

[...] n'entre certainement pas dans l'attente raisonnable des hôtes et de leurs invités que le prix de leur présence doit être leur consentement tacite à l'enregistrement électronique permanent, par des agents de l'État et à leur seule discrétion, des activités en cours.<sup>25</sup>

En 1990 également, la Cour suprême a dû se pencher sur un autre aspect des activités de surveillance électronique étatique. Les services policiers avaient obtenu l'autorisation judiciaire de placer une personne qu'elles soupçonnaient de trafic de stupéfiants sous surveillance, et avaient notamment mis sur écoute des téléphones situés dans des cabines publiques disposées près de lieux que le suspect fréquentait<sup>26</sup>. L'autorisation judiciaire accordée ne mentionnait toutefois pas cette dernière possibilité, bien que le juge en ait été informé<sup>27</sup>. Les informations obtenues par l'écoute de ces téléphones publics ont été en bonne part écartées, pour les motifs suivants:

[...] étant donné la large portée des autorisations, des centaines de conversations privées ont pu être

---

<sup>22</sup> *Ibid.*, 45-46.

<sup>23</sup> *Ibid.*, 47.

<sup>24</sup> *Ibid.*, 49-52

<sup>25</sup> *Ibid.*, 51.

<sup>26</sup> *R. c. Thompson*, [1990] 2 R.C.S. 1111.

<sup>27</sup> *Ibid.*, 1144.



enregistrées en l'absence d'aucune cible. Dans l'arrêt *Finlay and Grellette*, précité, l'autorisation exigeait la surveillance physique du téléphone public pour veiller à ce que les conversations ne soient interceptées que lorsqu'une cible l'utilisait. En l'espèce, il n'y a aucune disposition semblable ni aucune autre restriction. J'aurais cru à tout le moins qu'une telle autorisation prévoirait que les conversations dans un téléphone public ne seraient pas interceptées à moins qu'il n'existe des motifs raisonnables et probables de croire qu'une cible utilisait le téléphone au moment où le dispositif d'écoute a été mis en marche. Les policiers ne peuvent pas simplement installer un dispositif d'écoute et quitter les lieux en le laissant fonctionner systématiquement dans l'espoir qu'une cible se présentera. Dans certains cas, c'est ce qui s'est passé ici.

[...]

À mon avis, les interceptions effectuées conformément à ces autorisations, qui étaient simplement des recherches à l'aveuglette non fondées sur des motifs raisonnables et probables de croire que la cible utiliserait alors les téléphones publics, étaient abusives. [...]

[...] tout élément de preuve recueilli par suite des interceptions dans les téléphones publics en l'absence de motifs raisonnables et probables de croire qu'une cible utilisait le téléphone a été obtenu contrairement à l'art. 8.<sup>28</sup>

La Cour a ainsi fixé des balises importantes: sauf circonstances particulières, on ne doit pas effectuer de surveillance électronique à l'aveuglette, sans être assuré que les communications qu'on intercepte mettent bien en cause les personnes qu'on veut surveiller, et non des tiers.

On doit dire enfin un mot de l'arrêt *R. c. Plant*<sup>29</sup>, qui paraît marquer une dilution de la notion d'«attente raisonnable» en matière de protection de la vie privée. Une source anonyme ayant informé la police de Calgary que M. Plant exploitait chez lui une

---

<sup>28</sup> *Ibid.*, 1145-1146.

<sup>29</sup> *R. c. Plant*, [1993] 3 R.C.S. 281.

plantation de chanvre indien, les policiers ont consulté le dossier informatique de M. Plant détenu par son fournisseur d'électricité et ont constaté que sa consommation semblait anormalement élevée, ce qui constitue un indice bien connu de l'existence d'une telle plantation. Il importe de préciser que la consultation de ce dossier a été effectuée sans mandat, et dans des circonstances que décrit ainsi la Cour:

[...] l'agent Fair a utilisé, le 9 mars 1990, un terminal se trouvant dans la section des enquêtes du service de police de Calgary et qui était relié à l'unité centrale des services publics de la ville; grâce à ce terminal, la police pouvait, moyennant un mot de passe, vérifier la consommation d'électricité à une adresse donnée.<sup>30</sup>

Pour la majorité, le juge Sopinka a conclu que la consultation d'un tel dossier ne portait pas atteinte aux «valeurs sous-jacentes de dignité, d'intégrité et d'autonomie» que consacre l'article 8 de la *Charte canadienne* et qu'

[...] on ne saurait raisonnablement prétendre que les dossiers informatisés consultés dans la présente affaire, lesquels font état du niveau de consommation d'électricité dans une résidence, dévoilent des détails intimes de la vie de l'appelant, la consommation d'électricité ne révélant [sic] que très peu de chose du mode de vie ou des décisions privées de l'occupant de la résidence.<sup>31</sup>

C'est précisément à l'égard de cet aspect de l'affaire que la juge McLachlin (maintenant juge en chef) a inscrit sa dissidence, estimant au contraire que «[...] les dossiers faisant état de la consommation d'électricité peuvent [...] révéler combien de personnes habitent une maison et en dire long sur leurs activités.»<sup>32</sup>

On doit noter trois (3) choses à l'égard de l'arrêt *Plant*. D'une part, la lecture de la décision de la Cour suprême ne permet pas d'établir précisément la nature des éléments de preuve que pouvait évaluer la Cour pour déterminer si des dossiers de consommation d'électricité révèlent ou non des «détails intimes de la vie» des individus. Ensuite, le juge Sopinka s'inspire notamment d'un courant jurisprudentiel états-unien qui a conclu que le IV<sup>e</sup> amendement à la Constitution des États-Unis ne s'appliquait pas à des dossiers

---

<sup>30</sup> *Ibid.*, 285.

<sup>31</sup> *Ibid.*, 293.

<sup>32</sup> *Ibid.*, 302-303.

bancaires, alors que le droit canadien reconnaît depuis les années 1920 au moins un niveau de confidentialité élevé à l'égard de tels dossiers: le précédent choisi pour fonder le raisonnement du magistrat paraît donc un rien malheureux<sup>33</sup>.

Enfin, cette décision a été rendue en 1993, et donc bien avant l'adoption par le Parlement de la *Loi sur la protection des renseignements personnels et les documents électroniques*<sup>34</sup> et la sensibilisation croissante de la population à l'égard du caractère sensible de nombreux types de renseignements en était encore à ses débuts. Avec respect, on ne peut donc exclure que la Cour opérerait dans l'avenir pour la thèse de la juge McLachlin, plutôt que pour celle défendue par le juge Sopinka. Cela semble d'autant plus vraisemblable que les motifs de la décision rendue dans l'affaire *Plant* tranchent avec la conception de la protection de la vie privée élaborée dans des arrêts tels que *Dyment* ou dans d'autres affaires antérieures<sup>35</sup>.

Résumons. La surveillance électronique par l'État constitue *prima facie* une atteinte abusive et inconstitutionnelle à la vie privée des personnes<sup>36</sup>. Elle ne sera tolérable que lorsqu'elle aura été autorisée par un juge d'une cour supérieure, convaincu que d'autres méthodes d'enquête ne donneront pas des résultats adéquats et que cette méthode pourrait réussir<sup>37</sup>. Il y aura exception à ce principe dans les situations où les personnes surveillées n'auront pas une attente raisonnable de protection de leur vie privée; ces cas sont cependant circonscrits<sup>38</sup> et on tiendra compte du caractère subjectif de telle attente de la part de la personne surveillée<sup>39</sup>. Même lorsqu'une autorisation judiciaire est accordée, elle ne devrait pas donner lieu à une surveillance aveugle, mais bien à des actions ciblées visant directement les personnes qu'on veut surveiller<sup>40</sup>.

---

<sup>33</sup> On comparera à cet égard *United States v. Miller*, 425 U.S. 435 (1976) et *Tournier v. National Provincial and Union Bank of England*, [1924] 1 K.B. 461, que les tribunaux canadiens ont constamment appliqué en matière bancaire.

<sup>34</sup> L.R.C., c. c. P-8.6 (L.C. 2000, c. 5), ci-après également la «LPRPDÉ».

<sup>35</sup> On pense entre autres ici aux décisions de la Cour d'appel de l'Ontario et de la Cour suprême du Canada dans l'affaire *Glover v. Glover et al. (no. 2)*, (1981), 29 O.R. (2d) 401, conf. *sub. nom. Glover c. Bell Canada*, [1981] 2 R.C.S. 563, où il s'agissait de contraindre Bell Canada à fournir des renseignements relatifs à un des ses abonnés, ce qu'ont refusé d'autoriser la Cour d'appel ontarienne et la Cour suprême.

<sup>36</sup> *R. c. Duarte*, op. cit.

<sup>37</sup> *Ibid.*

<sup>38</sup> *R. c. Wong*, op. cit.; *R. c. Plant*, op. cit.

<sup>39</sup> *R. c. Duarte*, op. cit., 47.

<sup>40</sup> *R. c. Thompson*, op. cit.

Si la Cour suprême a souligné dans les arrêts précités le caractère absolument fondamental de la préservation du droit à la vie privée dans notre société, elle n'a pas manqué non plus d'insister depuis des décennies sur l'importance du respect de la liberté d'expression, dont la portée constitutionnelle est maintenant cristallisée dans l'alinéa 2 b) de la *Charte canadienne*<sup>41</sup>. On verra *infra* que ces certaines des propositions contenues dans le Document de consultation devront être évaluées aussi à la lumière du respect de cette liberté.

On doit dire également un mot d'un autre droit fondamental garanti, celui-là, par l'alinéa 11 c) de la *Charte canadienne*: il s'agit du droit pour un inculpé «de ne pas être contraint de témoigner contre lui-même dans toute poursuite intentée contre lui pour l'infraction qu'on lui reproche»<sup>42</sup>.

ii) l'évaluation selon l'art. premier

Cela dit, les droits conférés par la *Charte canadienne* ne sont pas absolus. Comme l'exprime son article premier, ils peuvent être restreints «par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique.» La portée de cette disposition a fait l'objet d'une abondante jurisprudence, que nous ne saurions ici examiner en détail. Il faut néanmoins en relever quelques faits saillants.

Certes, les lois bénéficient au Canada d'une présomption de constitutionnalité<sup>43</sup>. Cependant et lorsqu'un justiciable convaincra le tribunal qu'une loi<sup>44</sup> enfreint un droit garanti par la *Charte canadienne*, il appartiendra alors à l'État de démontrer que cette règle de droit est raisonnable et justifiable<sup>45</sup>. Il devra à cet égard se plier pour l'essentiel à un test qui comporte quatre branches<sup>46</sup>.

<sup>41</sup> et dont l'application la plus récente par la Cour suprême se trouve dans l'arrêt *Ruby c. Canada (Solliciteur général)*, 2002 CSC 75 (21 novembre 2002), où elle a triomphé dans une certaine mesure du vif goût du secret des autorités chargées de la protection de la sécurité nationale.

<sup>42</sup> Encore faudra-t-il que la Cour suprême détermine l'effet de cette disposition sur une tentative de mise en preuve d'éléments autres que des déclarations de l'accusé postérieures à sa mise en accusation, effet qui pourrait être assez limité si on juge par exemple par sa décision dans l'affaire *R. c. Fitzpatrick*, [1995] 4 R.C.S. 154.

<sup>43</sup> Notamment, *Nova Scotia Board of Censors c. McNeil*, [1978] 2 R.C.S. 662, 687-688.

<sup>44</sup> ou un autre acte étatique, bien sûr.

<sup>45</sup> *R. c. Oakes*, [1986] 1 R.C.S. 103, 136-137.

<sup>46</sup> *Ibid.*, 138-139.

D'abord, l'objectif législatif poursuivi doit s'avérer suffisamment important pour justifier une limitation à un droit garanti par la *Charte canadienne*. Ensuite, il doit exister un lien logique et rationnel entre l'objectif poursuivi et la règle de droit dont la constitutionnalité est contestée. En troisième lieu, l'atteinte au droit garanti doit être limitée au strict nécessaire requis pour atteindre l'objectif poursuivi et, enfin, la limitation contestée ne doit pas avoir sur les personnes touchées un effet disproportionné à l'objectif poursuivi.

Le troisième facteur a conduit depuis l'adoption de la *Charte canadienne* à l'invalidation de plusieurs lois, dans le domaine pénal comme dans d'autres secteurs<sup>47</sup>. Il s'agit donc d'un élément important qui doit être pris en compte dans l'évaluation d'une mesure législative dans un cas comme celui qui nous intéresse. La question se pose dès lors essentiellement dans les termes suivants: le Parlement aurait-il pu atteindre son objectif en établissant une mesure moins attentatoire au droit fondamental en cause?

Rappelons enfin que les tribunaux ont également signalé qu'une loi trop imprécise peut en principe être invalidée pour ce seul motif<sup>48</sup>. On sait d'autre part qu'il convient de rechercher (et de préférer) l'interprétation d'une disposition législative qui soit compatible avec une norme telle que la *Charte canadienne*<sup>49</sup>.

C'est dans ce cadre juridique que devront agir le Parlement et les services policiers afin de mettre en oeuvre les orientations proposées dans le Document de consultation. La seule lecture du Document de consultation ne permet certes pas d'acquérir la conviction qu'ils s'y conformeront sans peine. L'État entend en effet se doter de moyens de grande envergure, qui pourraient forcer les Canadiens à réviser radicalement ce qu'ils croient être des attentes raisonnables en matière de protection de leur vie privée dans le domaine des télécommunications.

## B- Les propositions étatiques

---

<sup>47</sup> Hogg, Peter. *Constitutional Law of Canada – 1998 Student Edition*. Toronto, Carswell, 1998. Pp. 724-726.

<sup>48</sup> *Ontario c. Canadien Pacifique Ltée*, [1995] 2 R.C.S. 1031; *Ruffo c. Conseil de la magistrature*, [1995] 4 R.C.S. 267; *Winko c. Colombie-Britannique (Forensic Psychiatric Institute)*, [1999] 2 R.C.S. 625, entre autres.

<sup>49</sup> Côté, P.-A. *Interprétation des lois*. 3e éd. Montréal, Thémis, 1999. Pp. 468-471; *Slaight Communications Inc. c. Davidson*, [1989] 1 R.C.S. 1038, 1078; *R. c. Thompson*, [1990] 2 R.C.S. 1111, 1158; *Ontario c. Canadien Pacifique Ltée*, *op. cit.*, 1051 (motifs concurrents du juge en chef Lamer).

Le Document de consultation formule des recommandations relatives à une dizaine de problématiques. On les examinera ici dans l'ordre où elles sont abordées dans le Document. On se penchera surtout sur les questions de fond qu'elles soulèvent, en ajoutant à l'occasion quelques éléments reliés aux questions particulières qui y sont posées. On conclura en disant un mot de certains éléments visés par la Convention sur la cybercriminalité, mais à l'égard desquels le Document de consultation demeure muet.

### 1- les modifications technologiques

On envisage dans le Document de consultation la possibilité d'obliger législativement les fournisseurs de service<sup>50</sup> à «s'assurer que leurs systèmes ont la capacité technique de fournir un accès légal aux organismes d'application de la loi et de sécurité nationale.»<sup>51</sup> En d'autres termes, les systèmes de communication doivent être conçus de telle manière que la surveillance ne soit pas impossible. La loi exigerait que les réseaux de communication soient poreux.

Cette hypothèse suscite un grand nombre de difficultés, dont certaines sont de l'ordre du principe et d'autres sont plus pragmatiques. Elles sont d'une ampleur telle qu'on peut douter que les objectifs visés puissent être atteints.

Il y a d'abord un paradoxe à exiger des équipementiers et des fournisseurs de services qu'ils déploient des services délibérément affaiblis, moins sécuritaires qu'ils ne pourraient l'être. On ne cesse d'exhorter entreprises et consommateurs à mettre en oeuvre des mesures de sécurité extrêmement élevées, mais les voies de circulation publique de l'information seraient délibérément vulnérables à certaines attaques. Il faudrait être d'un optimisme qui relève de la fabulation pour croire que seuls les organismes policiers et les agences chargées de la sécurité nationale canadiens seront capables d'exploiter ces failles. C'est là s'assurer de rendre vulnérable toute l'infrastructure de communication canadienne, au nom de son hypothétique protection.

C'est également menacer la sécurité des communications de chaque personne, y compris de celles qui n'ont rien à se reprocher. Bref, il s'agit d'une mesure qui porte

---

<sup>50</sup> i.e. les personnes qui possèdent ou exploitent des installations de transmission utilisées par elles-mêmes ou par un tiers pour fournir des services de télécommunications au public au Canada, selon la «définition ad hoc» qu'on trouve dans le Document de consultation, en p. 4.

<sup>51</sup> Document de consultation, *op. cit.*, p. 8.

atteinte aux droits et aux intérêts de tous les Canadiens et de toutes les entreprises canadiennes, qui en ignoreront pourtant pour la plupart la portée et les conséquences.

La proposition entraîne aussi, inévitablement, un frein à l'évolution technologique au Canada dans un domaine de pointe. En effet et même si des équipementiers, par exemple, inventaient de nouveaux systèmes plus performants et plus sécuritaires, ils ne trouveraient pas de marché pour ces produits au Canada. Accessoirement, ils ne trouveront peut-être guère de marchés étrangers pour leurs produits poreux non plus, les autorités d'autres États pouvant être réticentes à l'installation dans leur infrastructure nationale de communication de systèmes dont elles savent qu'ils peuvent en tout temps être percés par les autorités canadiennes.

La contrepartie n'est pas moins vraie: voudra-t-on que soient installés au Canada les systèmes conçus par des firmes françaises, allemandes, japonaises, qu'on saurait transparents pour les agences de sécurité nationale de ces États? Peut-être pas. Mais on ne pourra pas non plus installer ici des systèmes de fabrication étrangère très performants, mais qui seront «opaques». S'agit-il là d'une barrière commerciale déguisée, ou du moins involontaire?

Il s'agit donc de sacrifier à la boulimie informationnelle des services policiers la sécurité des réseaux et un pan appréciable de la politique industrielle canadienne. Le choix nous paraît mériter une réflexion sérieuse. Rappelons d'autre part qu'on n'a pas démontré à quel besoin impératif cette mesure devait répondre.

Tout se passerait un peu comme si, il y a quelques siècles, on avait prohibé l'usage de la colle sur les enveloppes pour s'assurer que les agents de la Chambre étoilée puissent lire le courrier de tous les sujets de Sa Majesté sans laisser de trace. On n'y pas songé — du moins, on ne l'a pas fait. Le précédent nous paraît mériter d'être suivi.

Se pose ensuite la question des coûts. Aux États-Unis, on a évalué que l'implantation de mesures analogues pourrait coûter au moins cinq cent millions de dollars<sup>52</sup>. On veut bien admettre que la proposition contenue dans le Document de consultation vise

---

<sup>52</sup> On sait qu'aux États-Unis, des coûts d'investissement de plus de 500 millions USD ont été évoqués au cours des dernières années pour mettre en place les systèmes requis par le *Communications Assistance for Law Enforcement Act* (ou «CALEA»), 47 USC 1001-1010, et plus précisément à cet égard § 1008. Cette loi fédérale a été adoptée en 1994. Beaucoup de commentateurs ont exprimé l'avis que les coûts d'implantation ont largement dépassé le budget alloué par le Congrès.

principalement les systèmes qui seraient mis en place dans l'avenir, et non les processus présentement utilisés. Il n'en reste pas moins qu'il faut s'attendre à des coûts de conception, d'implantation et d'utilisation qui pourraient être appréciables. Les fournisseurs de service seraient-ils dédommagés par l'État parce qu'ils lui facilitent la vie? Ces coûts seraient-ils plutôt refilés à des millions de consommateurs qui, pour la très grande majorité, ne posent aucun risque tel qu'il faudrait prendre de telles mesures<sup>53</sup>? On l'ignore.

On ne saurait non plus exclure que l'ampleur des investissements qui seraient requis puisse avoir un effet sur la concentration des entreprises dans le secteur de la fourniture de services de télécommunication. Les petits fournisseurs de service, par exemple, pourraient s'avérer financièrement incapables de s'acquitter des obligations qui leur seraient faites. Seuls les plus gros survivraient alors, ce qui pourrait avoir des incidences anticoncurrentielles non négligeables.

Le champ d'application de la mesure envisagée pose par ailleurs des problèmes extrêmement sérieux. D'abord,

[...] les fournisseurs de services seraient contraints d'avoir la capacité technique permettant d'accéder à toutes les données spécifiques transmises par leurs installations, y compris celles relatives au contenu d'une télécommunication et les données relatives à cette même télécommunication.<sup>54</sup>

Cette assertion soulève à elle seule deux difficultés graves: elle vise «toutes les données» transmises par un fournisseur, et elle inclut le contrôle du contenu. Envisageons-les tour à tour.

D'autres, qui connaissent plus finement toutes les subtilités techniques d'un réseau tel que l'Internet, sauront mieux que nous démontrer précisément ce qui paraît néanmoins indéniable: les communications circulant sur ce réseau transitent au moins à l'occasion par un grand nombre d'intermédiaires. La chose n'est pas moins vraie en matière de téléphonie: l'appel logé par un résident de San Francisco à un habitant de Fredericton

<sup>53</sup> Notons incidemment que la législation états-unienne prescrit quant à elle que l'impact des investissements requis sur le tarif des services téléphoniques résidentiels de base soit pris en compte dans la détermination des mesures qu'on peut raisonnablement mettre en oeuvre: CALEA, § 1008 (b) (1) (B).

<sup>54</sup> Document de consultation, *loc. cit.*



passer par un réseau local californien, un réseau interurbain états-unien, peut-être le réseau de Bell Canada et aboutit au réseau de la société Aliant Telecom Inc.: Bell, ou d'autres intermédiaires, devraient-ils être en mesure de fournir l'accès à des données provenant de réseaux étrangers et destinés à d'autres réseaux, et utilisant peut-être des technologies différentes? Devraient-ils avoir cette capacité même dans les cas où ni l'expéditeur, ni le destinataire d'une communication n'est leur abonné<sup>55</sup>?

À tout le moins, des distinctions devront sans doute être opérées entre le réseau d'origine d'une communication, le transitaire et le destinataire<sup>56</sup>. On imposerait autrement au fournisseur transitaire ou destinataire qui ne peut pas fournir aux autorités l'accès au contenu d'un message donné l'obligation légale de le constater, et de refuser d'acheminer ce message jusqu'à sa destination finale. On imagine les difficultés que cela susciterait au niveau de l'acheminement des messages et du respect de la liberté d'expression, et le fardeau administratif et financier qui serait de ce fait imposé aux entreprises de télécommunication qui, contrairement à leurs obligations légales déjà établies par ailleurs, se verraient contraintes d'effectuer une censure systématique à l'égard des messages<sup>57</sup> auxquels ils ne peuvent techniquement fournir l'accès qui serait requis. En effet, ils enfreindraient autrement la loi, en acheminant des communications sans pouvoir en permettre l'interception.

On a noté par ailleurs que cette obligation viserait les fournisseurs qui offrent des services de communication «au public». Cela pose une double difficulté. D'abord, il s'agit d'un champ bien moins clairement délimité qu'on pourrait le croire; ensuite, cette restriction pave la voie à l'évitement des mesures envisagées.

Qui, en effet, offre des services de communication au public? Les fournisseurs de services commerciaux comme Telus, Microcell ou Sympatico, bien sûr. Mais qu'en est-il d'une université qui permet à ses étudiants, et peut-être à tous les membres de la communauté, d'utiliser son réseau pour naviguer sur l'Internet? Qu'en est-il d'une grande métropole offrant un accès direct à l'Internet dans ses bibliothèques? Qu'en est-il du Réseau de télécommunications sociosanitaire du Québec, auquel pourraient être branchés tous les établissements de santé, mais aussi par exemple les cabinets des médecins? Qu'en

<sup>55</sup> Aux États-Unis le libellé législatif ne paraît pas exiger d'un fournisseur qu'il dispose d'une capacité d'interception des communications dont il n'est que le transitaire.

<sup>56</sup> On évoque la possibilité que des pouvoirs réglementaires soient attribués, qui permettraient d'établir des exemptions à l'obligation de garantir la capacité d'interception; on ignore évidemment à ce stade ce que pourraient être ces exemptions.

<sup>57</sup> On pense par exemple à l'article 36 de la *Loi sur les télécommunications*, L.R.C., c. T-3.4.

est-il des réseaux de communication des institutions financières, qui acheminent les instructions de paiement électronique provenant de tous les détenteurs de cartes de débit? Qu'en est-il du réseau informatique interne d'une firme transnationale quelconque, qu'utilisent aussi les employés pour naviguer sur l'Internet à des fins personnelles? Il y a là matière à des nuances nombreuses et subtiles, et à un choix dont les conséquences seront considérables<sup>58</sup>.

Car ou bien on assimile beaucoup de ces réseaux à des fournisseurs de service «au public», et on impose alors à de nombreux organismes un fardeau considérable, et peut-être démesuré<sup>59</sup>. Ou bien on les exempté, et on offre alors aux criminels l'occasion d'utiliser des réseaux non poreux, ou même de s'en constituer. Les honnêtes gens seraient alors susceptibles de voir leurs communications interceptées, mais les escrocs les plus habiles pourraient échapper en bonne part à la surveillance. Il s'agit d'une problématique qui ne pourrait être résolue qu'en jetant plus de clarté sur la portée précise des propositions gouvernementales.

D'autre part et quant au contrôle du contenu des communications traitées par ces fournisseurs, l'obligation de l'assurer est évoquée en termes vagues dans la description de la proposition gouvernementale. On y indique que les fournisseurs devraient avoir «la capacité technique permettant d'accéder [...] au contenu d'une télécommunication»<sup>60</sup>. Sans doute faut-il comprendre que là où le fournisseur offre lui-même un processus de chiffrement des communications, ce processus devra être assorti d'un sésame qui permettra aux autorités de déchiffrer sans peine les messages<sup>61</sup>.

C'est dire, évidemment, que les escrocs et les terroristes les plus habiles auront recours en plus à d'autres méthodes de chiffrement, dont on ne peut en pratique empêcher

<sup>58</sup> Beaucoup des institutions que nous avons évoquées peuvent en effet être branchées directement à l'Internet, sans passer par un fournisseur conventionnel. Aux États-Unis, le CALEA vise les *common carriers for hire*, ce qui paraît un peu plus précis que le libellé suggéré par le Document de consultation.

<sup>59</sup> Et on notera au passage qu'à titre d'élément contextuel, l'alinéa 14 (3) b. de la Convention sur la cybercriminalité militerait en faveur d'une interprétation extensive du type de réseaux à l'égard desquels on peut vouloir assurer une surveillance. En cas d'ambiguïté législative, les tribunaux canadiens interpréteront la disposition en litige en tenant compte des obligations internationales du Canada, même si elles n'ont pas été traduites dans la législation: *Daniels c. White et La Reine*, [1968] R.C.S. 517, 541; *National Corn Growers c. T.C.I.*, [1990] 2 R.C.S. 1324, 1371.

<sup>60</sup> Document de consultation, *loc. cit.*

<sup>61</sup> C'est du moins la teneur de la législation états-unienne: CALEA, § 1002 (b) (3).

l'utilisation; les grandes entreprises<sup>62</sup> ou les professionnels assujettis légalement au secret voudront aussi utiliser des méthodes de chiffrement offertes par d'autres que les fournisseurs de télécommunication, et qui auront la réputation d'être très difficiles à percer, parce qu'ils voudront ou devront légalement assurer la confidentialité des communications auxquelles ils participent.

Les criminels et les terroristes les plus habiles et les plus puissants<sup>63</sup> établiront pour leur part dans quelque petite île des Antilles ou du Pacifique le centre de leurs réseaux de communication, et ils transmettront leurs données ici et là dans le monde (y compris vers le Canada) grâce à des satellites qui pourraient bien un jour battre pavillon panaméen... et ils échapperont ainsi dans une large part aux velléités de contrôle canadien. À moins de censurer toute communication provenant de tels sanctuaires informationnels<sup>64</sup>, on aura donc simplement déplacé le problème.

L'objectif recherché ne sera donc vraisemblablement pas atteint, et les criminels assez maladroits pour communiquer en clair ou par des chiffres vulnérables auront sans doute commis bien d'autres bêtises qui auraient à elles seules mené à leur arrestation.

L'imposition du contrôle de l'accessibilité des contenus aux fournisseurs de service est donc pour l'essentiel vouée à l'échec<sup>65</sup>. À moins qu'elle aille, comme on l'a noté *supra*, jusqu'à l'interdiction de transmettre des messages qui ne peuvent être déchiffrés. Mais ce serait là imposer aux fournisseurs l'obligation de contrôler *a priori* la lisibilité potentielle des *tous* les messages qu'ils transmettent. Même en maintenant ce contrôle à sa plus simple expression<sup>66</sup>, il faut envisager les coûts qui en découleraient, les délais

---

<sup>62</sup> Et on rappellera qu'elles jouissent elles aussi de certaines attentes légitimes en matière de protection de leur «vie privée» en vertu de la Constitution canadienne: *Hunter c. Southam*, [1984] 2 R.C.S. 145

<sup>63</sup> et donc les plus dangereux.

<sup>64</sup> et on éprouvera quelque peine à bloquer celles qui sont transmises par satellite.

<sup>65</sup> si on la considère comme une obligation de résultat; on pourrait aussi n'y voir qu'une obligation de moyen, mais il faudrait alors obliger simplement les fournisseurs à prendre des moyens «raisonnables», comme on le fait aux États-Unis dans le CALEA ou, au Royaume-Uni, par le par. 11 (5) du *Regulation of Investigatory Powers Act 2000*, 2000 c. 23, encore que la notion de «moyens raisonnables» aux fins de cette dernière loi puisse être sujette à caution.

<sup>66</sup> ce qui peut se réaliser informatiquement de manière au moins approximative par des techniques d'analyse statistique sur des fragments de message qu'on a soumis à un processus de décryptage pour établir si la fréquence d'apparition de diverses lettres est comparable à celle qu'on observe dans des langues comme le français ou l'anglais, par exemple. Pour une introduction à cette question, on pourra lire Singh, Simon. *The Code book*. Doubleday, New York, 1999. Pp. 16-20.

d'acheminement des communications et l'intrusion potentiellement massive dans la vie privée de tous ceux qui échangent ces communications<sup>67</sup>.

Ce serait aussi faire payer les destinataires de messages légitimes, mais qu'un fournisseur ne peut décrypter, pour les choix cryptographiques de leurs correspondants. Et, pour assurer la transmission de leurs communications, ce serait obliger tous les acteurs sociaux à s'exprimer en clair ou en utilisant des techniques de chiffrement peu puissantes. Pour reprendre l'analogie du courrier conventionnel, ce serait remplacer toutes les lettres cachetées qui s'échangent dans le cours de la vie et des affaires par des cartes postales. Les citoyens, les entreprises, les professionnels, l'administration publique elle-même s'en indigneraient assurément; pourquoi devraient-ils alors le tolérer dans le domaine électronique?

D'autre part, la mesure envisagée aurait des conséquences sur la sécurité et le secret, mais aussi sur la liberté d'expression. On parle en droit états-unien de *chilling effect* pour évoquer l'effet inhibitif de certaines actions de l'État sur les débats publics, même dans des cas où ce n'est pas l'objectif visé<sup>68</sup>. Et si le concept vise d'abord les cas où la loi (ou une autre règle) pêche à ce point par ambiguïté que le justiciable ne peut déterminer si une communication serait ou non licite<sup>69</sup>, il inclut également ceux où la surveillance étatique intimide ceux qui veulent émettre ou recevoir des messages<sup>70</sup>. La Cour suprême du Canada a aussi fait écho à cette préoccupation dans l'arrêt *Duarie*, notamment<sup>71</sup>. Et on la retrouve également dans les décisions des instances européennes.

Ajoutons un élément important: parmi les facteurs contribuant à la liberté d'expression se trouve l'anonymat. La chose a été rappelée récemment par la Cour suprême des États-

---

<sup>67</sup> et le tout pourrait bien être vain: des techniques stéganographiques permettent par exemple de camoufler un texte dans une illustration de telle manière qu'il serait extrêmement laborieux de contrôler tous les messages pour s'assurer qu'ils ne contiennent pas, quelque part, un message à la fois encrypté et caché. Les logiciels stéganographiques en vente libre sur l'Internet abondent et on consultera par exemple, à titre purement illustratif, le site [www.neobytesolutions.com/invsecl](http://www.neobytesolutions.com/invsecl). Cela dit, on n'ignore pas que ces méthodes de camouflage comportent elles aussi leurs vulnérabilités. Il faut cependant envisager l'ampleur des investissements qui seraient requis des fournisseurs de service.

<sup>68</sup> Depuis *Schneider v. State*, 308 U.S. 147 (1939) au moins: à cet égard, cf. par exemple Tribe, Laurence H. *American Constitutional Law*. 2d Edition. Mineola, Foundation Press, 1988. Pp. 978 ss.

<sup>69</sup> *Ibid.*, 1022 ss., et notamment 1033 ss.

<sup>70</sup> On pense par exemple aux arrêts *Lamont v. Postmaster General*, 381 U.S. 301 (1965), *United States v. United States District Court*, 407 U.S. 297 (1972), notamment aux pp. 314-315 et *Reno v. ACLU*, 117 S.Ct. 2329, 138 L.Ed. 2d 874 (1997).

<sup>71</sup> *op. cit.*, 44, précité.

Unis<sup>72</sup>. On peut croire que les tribunaux canadiens en viendraient à une conclusion semblable<sup>73</sup>. Or il va de soi que les mesures envisagées en matière d'établissement de capacités technologiques d'interception iraient absolument à l'encontre de la capacité pour un internaute, par exemple, de communiquer anonymement ou de consulter sans être identifié des sites web exprimant certains points de vue.

Or, outre l'effet qu'aurait cette conséquence sur la liberté d'expression, elle limiterait également sérieusement les choix en matière commerciale. On sait en effet qu'on été conçus des mécanismes informatiques extrêmement fiables qui permettent à des parties de confirmer à distance leur droit à une prestation sans s'identifier formellement. Cela permet de préserver dans le monde virtuel l'anonymat commercial dont nous jouissons présentement dans le monde physique, sans compromettre la sécurité et l'efficacité des opérations<sup>74</sup>. Des exigences imposant des capacités d'interception trop détaillées pourraient prohiber le déploiement de telles techniques.

L'implantation des envisagées mesures aurait pourtant vraisemblablement pour effet, si elles fonctionnaient, d'interdire aux Canadiens d'utiliser des services offrant l'anonymat sur l'Internet<sup>75</sup>: les services les plus efficaces font en effet en sorte qu'on ne peut établir l'identité de l'anonymographe, parce que des données relatives à la communication ne peuvent être obtenues ou déchiffrées par un intercepteur.

Bref, un polémiste, un pamphlétaire seraient tentés de lancer qu'on se trouverait avec les propositions gouvernementales bien près de ramener la liberté d'expression et de commerce de l'internaute canadien au rang de celle de l'internaute chinois. Bornons-nous à constater que ces propositions manquent tant de précision qu'elles ouvrent la porte à toutes les interprétations.

---

<sup>72</sup> *Watchtower Bible & Tract Society of New York v. Village of Stratton*, une décision unanime (et la chose est assez rare pour qu'on le souligne) de la Cour suprême des États-Unis rendue le 17 juin 2002. L'appelant contestait la validité d'un règlement municipal exigeant l'obtention d'un permis pour passer de porte en porte et a eu gain de cause.

<sup>73</sup> Et, avant même l'adoption de déclarations des droits constitutionnelles ou quasi-constitutionnelles, la Cour suprême avait (à la majorité) cassé un règlement municipal imposant l'obligation d'obtenir la permission écrite du chef de police avant de pouvoir distribuer des documents dans les rues de la ville de Québec: *Saumur c. Cité de Québec*, [1953] 2 R.C.S. 299. Le parallèle avec la récente décision états-unienne dans l'affaire *Watchtower* paraît flagrant.

<sup>74</sup> À l'égard de ces questions, on consultera par exemple Brands, Stefan. *Rethinking Public Key Infrastructures and Digital Certificates – Building in Privacy*. Cambridge, MIT Press, 2000. 314 p.

<sup>75</sup> comme le service offert au [www.anonymizer.com](http://www.anonymizer.com), pour ne fournir que cet exemple.

Or la protection de la vie privée sur l'Internet comporte une dimension particulière, et peut-être tout à fait nouvelle dans l'Histoire. Le même instrument sert en effet non seulement au courrier, mais à la publication au bénéfice d'un public illimité et à la consultation de tout ce qui est ainsi publié. Il sert aussi à effectuer des opérations commerciales. L'internaute peut être à la fois épistolier, éditeur, libraire, chercheur, lecteur, auditeur, consommateur... Et c'est de l'ensemble de ces activités, dont la saisie peut servir à brosser un portrait extraordinairement précis de ses activités, de ses réseaux et de sa vie, qu'on veut capter les traces. L'impact social et juridique d'une telle initiative dépasse largement celui de l'interception du courrier ou des appels téléphoniques, ou la surveillance du domicile: il les inclut et comprend aussi nombre d'autres dimensions. Or on n'a jamais imposé aux infrastructures postales et téléphoniques d'être poreuses et capables de déchiffrer tous les messages qu'elles transmettent, alors qu'on veut le faire aujourd'hui pour l'Internet.

En somme, on voudrait légalement forcer le sabotage de la sécurité des communications. Et on espère qu'aucun escroc, aucun terroriste n'en profitera<sup>76</sup>. Les conséquences d'une telle mesure s'imposeraient à tous les Canadiens, ainsi qu'à une de nos principales industries, pour une période indéterminée. La preuve de l'efficacité d'une telle mesure n'est par ailleurs pas encore rapportée, non plus que celle des circonstances qui la requièrent. On voit donc mal comment on convaincrat les tribunaux qu'il s'agit d'une limite raisonnable à des droits fondamentaux, qui impose une atteinte limitée au strict nécessaire requis pour atteindre l'objectif recherché. On se sent bien loin de la protection accordée dans l'ordre du principe contre les fouilles, les perquisitions et les saisies abusives par l'article 8 de la *Charte canadienne*<sup>77</sup>.

Notons au passage qu'on se trouve donc ici dans cette étrange situation où on tente de tenir un débat public et démocratique à l'égard de questions complexes en soumettant aux intéressés moins d'éléments de preuve qu'il n'en faudrait pour convaincre un tribunal canadien du bien-fondé des mesures dont il s'agit. Il y a là l'ombre d'une anomalie.

Peut-être maladroitement, le Document de consultation formule la position ministérielle tout comme s'il s'agissait de constituer aux fournisseurs de service une obligation de résultat: ils doivent rendre l'interception possible, quoi qu'il en coûte<sup>78</sup>. Cette

---

<sup>76</sup> même si on ne sait pas quelles mesures technologiques on déploierait pour les en empêcher, ou dans quelle mesure on détecterait des intrusions non autorisées.

<sup>77</sup> *Dyment, op. cit.*, p. 427.

<sup>78</sup> financièrement et autrement.

orientation paraît foncièrement irréaliste et excessivement attentatoire aux droits fondamentaux. Il faut espérer que l'énoncé de cette position dans le Document de consultation traduise mal les orientations du gouvernement, mais nous n'avons d'autre choix à ce stade que d'analyser le projet soumis à la consultation, et d'en souligner à gros traits les failles les plus flagrantes.

Dans ce contexte, les «questions à examiner» formulées dans le Document de consultation<sup>79</sup> manquent singulièrement de perspective. Elles fournissent toutefois des indications inquiétantes quant à l'ampleur du monstre bureaucratique qu'on pourrait créer. La formulation de règlements relatifs aux normes auxquelles les fournisseurs de service devraient se plier constituera par exemple un défi de taille, à moins que ces règlements se bornent à des énoncés généraux qui ne permettront pas à ces fournisseurs de déterminer facilement comment s'y conformer.

Autre élément important, on envisage des consultations avec les fournisseurs concernés et, sans doute, d'autres intervenants de l'industrie. Il serait incompréhensible qu'on n'associe pas à ces processus des représentants des citoyens et la communauté juridique, dont l'éclairage pourrait contribuer grandement aux débats. Il paraît en effet préférable à tous égards de prendre en compte les points de vue du public au moment de la conception des systèmes, plutôt que d'avoir à rebâtir ces derniers à grand coût parce qu'un tribunal les a jugés attentatoires aux droits fondamentaux<sup>80</sup>.

Par ailleurs, on s'inquiète au plus haut point de la possibilité que des règlements balisent «la compétence, la fiabilité et la mise en place du personnel»<sup>81</sup>. Faut-il comprendre que toute personne oeuvrant pour un fournisseur de service pourrait devoir être contrainte à l'obtention d'une attestation de sécurité? Qu'un non-citoyen, ou une personne détenant un casier judiciaire pour une peccadille, pourrait être légalement empêché d'oeuvrer au sein d'un fournisseur de services, parce qu'il pourrait constituer un risque? Il s'agirait là d'une immixtion peut-être sans précédent en temps de paix dans la gestion de la main-d'oeuvre dans le secteur privé au Canada. On ne sache pas qu'il existe présentement de telles obligations légales imposées aux entreprises de télécommunication, ou aux banquiers, ou aux équipementiers et aux concepteurs de logiciels, ou aux firmes de génie-conseil qui conçoivent des ponts ou des centrales

<sup>79</sup> *op. cit.*, pp. 9-10.

<sup>80</sup> La législation états-unienne envisage d'ailleurs la consultation des usagers: CALEA, § 1006 (a) (1).

<sup>81</sup> *Ibid.*, p. 10.

nucléaires. Mais on pourrait imposer à un libertel<sup>82</sup> d'effectuer une enquête de sécurité avant d'embaucher un technicien en informatique. La démesure est flagrante entre le risque allégué (ou perceptible) et le caractère intrusif de la mesure, qui devrait être rayée du catalogue des pouvoirs réglementaires susceptibles d'être accordés.

Le Document de consultation contient par ailleurs peu de précisions quant aux mécanismes de conformité qui pourraient être mis en place pour garantir le respect de l'obligation de garantir la capacité d'interception qu'on voudrait établir légalement. Il paraît peu utile de spéculer à ce stade sur les formes qu'ils pourraient prendre, tout scénario qu'on pourrait esquisser pouvant n'avoir rien de commun avec ce qu'envisagent les autorités gouvernementales.

Il faut cependant mettre l'accent sur un aspect de ces éventuels mécanismes de contrôle: leur mise en oeuvre ne doit en aucune manière et à aucun prix être confiée aux corps policiers ou aux organismes chargés de la sécurité nationale qui bénéficieraient des capacités d'interception ainsi constituées, ni à des organes qui leur seraient liés ou qui relèveraient des mêmes ministres de tutelle. Ce serait en effet confier au loup l'inspection des serrures de la bergerie. Ces organismes n'auraient de cesse de suggérer qu'on pourrait se conformer encore mieux aux obligations de garantie de la capacité d'interception en minant de toutes les manières les quelques remparts protégeant encore la vie privée des citoyens, afin qu'ils puissent plus facilement envahir la forteresse. Il n'y aurait pas là malice, mais simplement volonté de ces organismes de n'être pas empêchés de remplir leur mission tels qu'ils la conçoivent. Ce n'est pas sans raison que la législation états-unienne en cette matière établit qu'une ordonnance de conformité ne peut être rendue que par un tribunal, et à des conditions précises<sup>83</sup>.

On notera aussi au passage qu'on laisse entendre dans le Document que la préparation des projets de règlement découlant de l'initiative législative dont il s'agit ressortirait au ministre de l'Industrie et au Solliciteur général<sup>84</sup>; il paraît regrettable qu'on veuille omettre

---

<sup>82</sup> Rappelons que les libertels (ou *freenets* en anglais) forment un réseau dont la «mission consiste à démocratiser l'accès aux technologies Internet dans des perspectives communautaire et éducative», pour reprendre le libellé utilisé au [www.libertel.org](http://www.libertel.org). Il s'agit donc d'organismes sans but lucratif, le plus souvent de petite taille et disposant de fort peu de ressources financières.

<sup>83</sup> CALEA, § 1007.

<sup>84</sup> *loc. cit.*



de ce processus le ministre de la Justice, pourtant garant en principe de la conformité de l'action gouvernementale à la *Charte canadienne*<sup>85</sup>.

Bref, on hésite quant à l'épithète qui qualifie le mieux la proposition d'instaurer une obligation légale de faciliter l'interception des communications imposée à tous les fournisseurs. Elle est kafkaïenne, orwellienne, chimérique, inquisitoriale, gratuite, rétrograde, totalitaire — et peut-être bien inconstitutionnelle... Elle procède de la philosophie que le progrès technologique ne doit rien ôter au pouvoir du souverain<sup>86</sup>, et devrait peut-être ne servir que lui. Elle n'a pas sa place dans la société canadienne du vingt-et-unième siècle.

Certes, on voudra objecter que cette capacité d'interception ne pourra être utilisée que dans les cas où les autorités auront obtenu un mandat judiciaire en bonne et due forme, qui leur permettra de consulter diverses données. Mais c'est là tenter d'éluder l'objet même du débat. Il s'agit d'imposer à tous les Canadiens de vivre dans une maison de verre, au motif que les policiers voudraient à l'occasion observer ce qui se passe lorsqu'ils croient qu'un crime pourrait être en voie d'y être ourdi. Ce n'est pas parce que les policiers devraient obtenir un mandat spécifique pour épier licitement ce qui se passe dans leur demeure que les Canadiens s'en trouveraient rassurés.

En somme, c'est rendre impossible la protection de la vie privée, et inhiber gravement la liberté d'expression. C'est ouvrir la porte à l'État orwellien, où le sujet sait seulement que chaque geste qu'il pose<sup>87</sup> peut être épié, sans même pouvoir établir s'il l'est ou non.

#### **Recommandation 2**

**Nous recommandons instamment qu'on n'établisse pas en droit canadien une obligation aux fournisseurs de service de garantir la capacité d'interception de toutes les télécommunications et que, si une telle obligation devait malgré tout être constituée, elle soit très rigoureusement balisée, notamment au plan des modalités, du partage des coûts, des circonstances dans lesquelles l'État peut en tirer parti et de la divulgation de son impact à toute la population.**

#### **2- les ordonnances générales de production**

<sup>85</sup> Sans doute serait-il consulté, mais il conviendrait qu'il participe directement à la genèse de tels règlements, si jamais le pouvoir de les édicter devait être accordé.

<sup>86</sup> de sorte qu'il peut faire l'économie de la recherche de nouvelles idées qui lui permettraient de s'adapter lui aussi au progrès, au lieu de le bloquer.

<sup>87</sup> ou, en l'occurrence, chaque communication envoyée ou reçue.

Dans la terminologie retenue dans le Document de consultation, une ordonnance de production «exige que le possesseur des documents remette ces documents à certaines personnes (comme les agents chargés d'appliquer la loi) dans un délai précis, ou les mette à leur disposition.»<sup>88</sup> On envisage d'accorder aux autorités la faculté d'obtenir trois (3) types de telles ordonnances. On s'arrêtera d'abord à l'ordonnance générale de production de documents.

Dans l'esprit du Document de consultation, une telle ordonnance paraît constituer à certains égards un substitut au mandat de perquisition, qui ne serait toutefois pas grevé de certaines des contraintes associées à l'obtention et l'exécution d'un tel mandat. Elle aurait pour effet que la personne visée devrait fournir les renseignements visés au bénéficiaire de l'ordonnance.

On peut *a priori* concevoir qu'une telle procédure puisse comporter une certaine utilité. Il n'aurait toutefois pas été inutile que le Document de consultation expose plus précisément les raisons pour lesquelles ce nouveau remède serait utile et les modalités qui seraient envisagées. Il faut également prendre garde à un certain nombre de difficultés qui seraient associées à l'émission de telles ordonnances.

On notera d'abord que le Document de consultation en dit qu'elles viseraient des «documents»; mais qu'entend-on par cette notion? Les écrits et les documents informatiques y seront selon toute vraisemblance inclus. En va-t-il de même d'enregistrements sonores ou visuels, de relevés biométriques, d'un outil de travail se trouvant sur le bureau d'un employé et qui porte à sa surface des identifiants biométriques...<sup>89</sup>? Voilà une notion qui devra impérativement faire l'objet de clarifications, puisque la technologie n'a présentement de cesse qu'elle permette d'extraire du sens et de l'information des sources les plus chaotiques ou les plus ténues. Tout support d'information pourra-t-il être assimilé à un «document»?

L'ordonnance de production vise ensuite la personne «en possession» de documents. Il faudra là aussi préciser ce qu'on entend par ce concept. Au strict plan juridique, la notion de «possession» en *common law* n'est pas réputée pour sa limpidité, et elle peut à certains

<sup>88</sup> Document de consultation, *op. cit.*, p. 11.

<sup>89</sup> qu'il s'agisse par exemple d'empreintes digitales ou de cellules corporelles contenant des molécules d'acide désoxyribonucléique.

égards différer de la notion de possession en droit civil<sup>90</sup>, également pertinente au moins à l'égard d'affaires en provenance du Québec parce qu'il n'y a pas à proprement parler de *common law* fédérale au Canada, sauf stipulation législative ou quant à ce qui relève du droit public<sup>91</sup>. À cela s'ajoute la difficulté que la possession du support et la «propriété» des informations qu'il contient peuvent ne pas coïncider exactement, de sorte qu'on peut par exemple entrer en possession des informations sans droit, mais sans les avoir volées ni avoir volé leur support<sup>92</sup>.

Au plan factuel, la possession de supports informationnels peut aussi soulever des difficultés embêtantes. Qu'en est-il, par exemple, du contenu d'une page web se trouvant très provisoirement dans la mémoire-tampon des systèmes de transmission d'un fournisseur de télécommunication qui ne sert que de transitaire? S'agit-il d'un «document» dont ce fournisseur est «en possession»? L'entreprise qui fournit un ordinateur portable à son représentant commercial (qui n'est peut-être même pas un salarié) est-elle «en possession» des informations se trouvant dans cet ordinateur, y compris les dossiers personnels du représentant qu'elle l'autorise dans une certaine mesure à y conserver?

L'entreprise canadienne dont une filiale exclusive située à l'étranger détient un document serait-elle elle-même présumée en possession de ce document, aux fins de l'exécution d'une ordonnance de production émise par un tribunal canadien<sup>93</sup>? La réponse serait-elle différente s'il s'agissait d'information «appartenant» à l'entreprise-mère, mais stockée sur des supports physiques appartenant juridiquement à la filiale étrangère? On pourrait multiplier les exemples qui illustrent à quel point il sera important de bien circonscrire la portée que pourraient avoir ces ordonnances.

Le mécanisme qu'on envisage de mettre en place paraît d'autre part avoir pour effet délibéré de contourner dans une certaine mesure les limitations que le Parlement se

---

<sup>90</sup> qui requiert qu'il y ait volonté d'exercer un droit réel sur le bien en cause, à défaut de quoi il n'y a que détention: *Code civil du Québec*, art. 921.

<sup>91</sup> *Q.N.S. Paper Co. Ltd. c. Canadien Pacifique Ltée*, [1977] 2 R.C.S. 1054, 1065-6; *Q.N.S. Paper Co. Ltd. c. Chartwell Shipping Ltd.*, [1989] 2 R.C.S. 683; *Roberts c. Canada*, [1989] 1 R.C.S. 322, 327, ce qui n'interdit évidemment pas de rechercher une certaine harmonisation entre les deux systèmes juridiques: *Banque de Nouvelle-Écosse c. Angelica-Whitewear Ltd.*, [1987] 1 R.C.S. 59.

<sup>92</sup> *R. c. Stewart*, [1988] 1 R.C.S. 963; *Cadbury Schweppes Inc. c. Aliments FBI ltée*, [1999] 1 R.C.S. 142.

<sup>93</sup> Une réponse positive tendrait à nier la pluralité des personnes juridiques en cause, ce qui pourrait avoir de nombreux effets juridiques imprévus en droit canadien comme en droit étranger; une réponse négative permet évidemment d'éluder en bonne part l'effet pratiquement extraterritorial qu'on voudrait donner à ces ordonnances, question à laquelle on revient à l'instant, en multipliant les filiales.

reconnaît généralement lorsqu'il s'agit de conférer un effet extraterritorial à ses lois<sup>94</sup>, ou que pose le droit international public en cette matière. Il est par exemple acquis qu'un État ne peut en principe imposer la mise en oeuvre de ses propres lois sur le territoire d'un autre État<sup>95</sup>. Les principes de courtoisie internationale militent aussi en faveur de la limitation volontaire de cet effet<sup>96</sup>. En fait, on admet généralement qu'une loi canadienne<sup>97</sup> ne comporte pas un effet extraterritorial, à moins qu'elle n'indique expressément avoir un tel effet<sup>98</sup>.

Les tribunaux canadiens s'efforcent également de limiter l'effet extraterritorial potentiel de leurs ordonnances, suivant en cela l'exemple britannique<sup>99</sup>. On n'en admettra pas moins que des situations comportant une dimension internationale puissent néanmoins être soumises aux tribunaux nationaux, même en matière pénale<sup>100</sup>.

Or il s'agit ici d'ordonner au Canada à une entité qu'on présumera susceptible d'être sanctionnée par un tribunal canadien<sup>101</sup> d'obtenir pour le compte des autorités canadiennes des documents qui peuvent se trouver sur le territoire d'autres États. Les autorités canadiennes n'ont de ce fait pas à obtenir la collaboration des autorités étatiques

<sup>94</sup> Le Canada constituant un État souverain, il peut conférer un effet extraterritorial à ses lois: *Croft v. Dunphy*, [1933] A.C. 156 (C.P.); il l'a d'ailleurs validement fait à l'occasion, comme les tribunaux l'ont reconnu: par exemple, *R. c. Finta*, (1989) 69 O.R. (2d) 557, 577, 580. conf. [1994] 1 R.C.S. 701.

<sup>95</sup> Brownlie, I. *Principles of Public International Law*. 3d Ed. Oxford, Clarendon Press, 1979. P. 310.

<sup>96</sup> quant au rôle de ces principes en droit canadien, par exemple, *U.S. District Court c. Royal American Shows*, [1982] 1 R.C.S. 415, 421; *Spencer c. La Reine*, [1985] 2 R.C.S. 278, 283.

<sup>97</sup> il s'agit évidemment des lois fédérales, les provinces ne disposant pas du pouvoir d'adopter des lois ayant un effet extraterritorial: *Statut de Westminster*, 22 Geo V, c. 44 (R.-U.), art. 4 (1931).

<sup>98</sup> comme, par exemple, la *Loi sur les sanctions économiques contre l'Iran*, L.C. 1980-81-82-83, c. 39, art. 3.

<sup>99</sup> On notera au passage que les autorités états-uniennes font preuve de beaucoup moins de timidité lorsqu'il s'agit de se prévaloir l'effet extraterritorial de leurs lois ou des autres actes de puissance publique: par exemple, *United States v. Alvarez-Machain*, 504 U.S. 655, 119 L. Ed 2d 441 (1992), où on a admis la licéité en droit états-unien de l'arrestation au Mexique d'un citoyen mexicain par les autorités états-uniennes (et son transport expéditif aux États-Unis pour le contraindre à y subir un procès pour meurtre), le tout sans le consentement des autorités mexicaines.

<sup>100</sup> Au Canada, *Spencer, op. cit.*, par exemple; en droit britannique, *D.P.P. v. Stonehouse*, [1978] A.C. 55 (H.L.).

<sup>101</sup> et qui a donc son domicile ou des biens au Canada, par exemple.

étrangères et la communication de ces renseignements peut même échapper entièrement au contrôle de ces autorités, qui n'en seront sans doute en aucune manière informées<sup>102</sup>.

On place donc le sujet de droit canadien dans ce qui pourrait devenir un dilemme cornélien. Les autorités canadiennes lui ordonnent ici de fournir, au pays, des «documents» qu'il «possède», mais qui se trouvent à l'étranger. Il se peut qu'il ait ce faisant à enfreindre au moins l'esprit du droit étranger. Il prive tout probablement les personnes<sup>103</sup> à l'égard desquelles des renseignements se trouvent dans ces documents des protections que le droit étranger pourrait leur procurer à l'égard d'une perquisition effectuée là où se trouvent les documents.

En somme, on privatise le processus de perquisition: le possesseur des documents fait lui-même le travail, au lieu qu'il soit accompli par un agent de l'État. Et cela permet d'exporter plus facilement l'activité de recherche et d'obtention d'information. L'entreprise<sup>104</sup> devient l'auxiliaire de l'État; elle agit comme un policier.

Et cela pose une question intéressante au plan du droit constitutionnel et administratif: cet auxiliaire de la puissance publique se trouve-t-il, du fait de ce qui constitue presque une délégation de pouvoir, assujéti à cette fin aux règles du droit public<sup>105</sup>, de façon à ne pas priver les citoyens des garanties juridiques dont ils jouiraient si l'État lui-même agissait, ou demeure-t-il un pur sujet de droit privé? Dans le premier cas, on impose implicitement à ces agents occasionnels de l'État un fardeau dont ils n'ont certes pas l'habitude, et on peut douter que les tribunaux retiendraient cette analyse. Mais dans le second, le détective privé amateur prend le relais du policier, sans que son activité soit encadrée de quelque manière que ce soit. Il n'y a là rien pour rassurer le citoyen.

Cette appréhension se justifie d'autant qu'on ne trouve rien dans le Document de consultation qui vienne baliser ce qu'on attendrait précisément de ceux à qui on signifierait une ordonnance de production de documents. Quel zèle doivent-ils mettre à découvrir les informations qu'on leur demande? Peuvent-ils se contenter d'efforts «raisonnables», ou doivent-ils remuer ciel et terre pour trouver ce qu'on leur demande? À

---

<sup>102</sup> On se souviendra au passage que le Canada a déjà légiféré afin d'éviter justement que des autorités étrangères puissent allègrement obtenir des éléments de preuve au Canada: *Loi sur les mesures extraterritoriales étrangères*, L.R.C., c. F-29.

<sup>103</sup> canadiennes ou étrangères.

<sup>104</sup> Les entreprises seront le plus souvent l'objet de ces ordonnances, puisqu'elles détiennent (hors certains organismes publics) la plus grande quantité de documents et d'informations.

<sup>105</sup> y compris l'obligation d'agir équitablement, de se conformer à la *Charte canadienne*...

quelle obligation de compétence sont-ils assujettis et qu'arrive-t-il si, de bonne foi, un possesseur de certains documents ne les trouve pas et ne les produit donc pas?

Il ne faut pas négliger non plus ce fait que, selon la nature des informations requises, la recherche et l'analyse de données par le destinataire de l'ordonnance peut requérir un travail considérable<sup>106</sup>; le destinataire pourra dès lors être tenté de remettre en vrac la botte de foin aux policiers, en les invitant à y chercher eux-mêmes l'aiguille — mais en divulguant ce faisant bien plus d'information, y compris des données relatives à des tiers, que n'en demande l'ordonnance.

Et cela repose accessoirement la question des coûts reliés à l'exécution d'une ordonnance: son destinataire sera-t-il indemnisé par l'État du fait qu'il effectue du travail policier pour le compte des agences de sécurité publique?

Il se peut bien que les auteurs du Document de consultation aient en tête des réponses claires, et peut-être même convaincantes, à l'égard de ces questions. Mais comme ils ne les ont pas encore fournies, force est de les poser à ce stade. Et, faute de les connaître, de tenir que la preuve n'a pas été faite jusqu'à maintenant que la création d'un régime tel que celui des ordonnances générales de production était nécessaire en droit canadien, ni qu'on pouvait encadrer adéquatement l'activité des entités qui seraient obligées de produire des documents.

### **Recommandation 3**

**Compte tenu des informations présentement disponibles, nous recommandons que ne soit pas établi en droit canadien le pouvoir d'obtenir des ordonnances générales de production.**

Parmi les «questions à examiner» à l'égard de ces ordonnances, le Document de consultation fait par ailleurs allusion à des «ordonnances anticipatoires», qui permettraient «de surveiller les transactions pendant un certain temps»<sup>107</sup>. On ne présente aucune justification à l'égard de l'établissement de telles ordonnances. On ne sait pas en vertu de quelles exigences procédurales elles pourraient être accordées, ni comment on

<sup>106</sup> Imaginons, par exemple, le cas d'une banque à qui on demande de retracer toute l'information relative aux paiements reçus depuis deux ans par un de ses clients, une entreprise qu'on soupçonne d'être contrôlée par le crime organisé, qui perçoit des paiements par chèque, par carte de crédit et par carte de débit et qui exploite des établissements dans 6 provinces canadiennes et trois États aux États-Unis. L'enquête peut fort bien être légitime, mais le travail requis de la part du banquier sera considérable.

<sup>107</sup> Document de consultation, *op. cit.*, p. 12.

surveillerait, ni pendant combien de temps. Et on ne peut que craindre que leur usage immodéré puisse mener en pratique à des pratiques assimilables à la rétention de renseignements. À la lecture du Document de consultation, il y a donc absence totale de fondement justifiant la création d'un tel instrument.

En ce qui a trait aux garanties procédurales dont devrait être assortie l'émission d'une ordonnance de production, il va de soi qu'elles devraient requérir une décision judiciaire, fondée sur la démonstration qu'il existe des motifs raisonnables de croire qu'une infraction a été commise ou est susceptible de l'être, et qu'il s'agit pour les autorités du moyen le plus efficace pour constituer la preuve requise aux fins d'une mise en accusation. Il devrait y avoir obligation légale que la portée de l'ordonnance soit strictement limitée quant aux autorités qui peuvent s'en prévaloir, quant aux types d'infractions à l'égard desquelles les éléments de preuve obtenus pourraient être utilisés, quant à la nature des documents, quant aux personnes visées, quant à sa durée et quant au territoire sur lequel elle peut être exécutée, notamment si on envisage que le destinataire soit requis de produire des documents se trouvant à l'étranger. Dans ces cas, l'ordonnance devrait requérir que les autorités étrangères soient informées de l'exécution de l'ordonnance avant que le destinataire transmette les documents visés. Enfin, les cibles visées devraient être informées qu'une ordonnance les concernant a été exécutée dans un délai raisonnable suivant la production des documents en cause.

### 3- les ordonnances spécifiques de production

On envisage également dans le Document de consultation<sup>108</sup> la création d'une nouvelle «ordonnance spécifique de production», qui constituerait dans une certaine mesure une extension des actuelles ordonnances émises, par exemple, en vertu des articles 487.01 et 492.2 du *Code criminel* et qui pourrait être obtenue par les autorités sans qu'elles aient à démontrer qu'elles ont des motifs raisonnables de croire qu'une infraction a été ou sera commise<sup>109</sup>. Cette ordonnance viserait essentiellement les «données relatives aux télécommunications», c'est-à-dire

---

<sup>108</sup> *Op. cit.*, pp. 12-13.

<sup>109</sup> et on notera au passage que ces 2 dispositions du *Code criminel* requièrent qu'il y ait des motifs raisonnables de croire (ou de «soupçonner», à l'art. 492.2) qu'une infraction a été ou sera commise; dans leur état actuel, elles n'appuient donc pas l'argument qu'il conviendrait de fixer un seuil moins élevé pour obtenir une ordonnance, à moins qu'on démontre que ces mécanismes ne fonctionnent pas adéquatement, démonstration qu'on ne trouve évidemment pas dans le Document de consultation.

toute donnée, y compris les données relatives aux fonctions de composition, d'acheminement, d'adressage ou de signal qui identifient ou visent à identifier l'origine, la direction, l'heure, la durée ou la taille, selon le cas, ainsi que le destinataire ou le point d'arrivée d'une transmission par télécommunication, générée ou reçue au moyen de l'installation de télécommunications exploitée par le fournisseur de services ou une installation lui appartenant.<sup>110</sup>

L'exigence d'un critère d'évaluation moins élevé à l'égard de l'émission d'ordonnances visant ces données s'expliquerait du fait qu'on leur associe une attente plus faible en matière de protection de la vie privée qu'à l'égard d'autres types de données.

On doit cependant souligner que cette justification ne tient pas. Elle tend d'abord à ignorer ce fait que de telles données fournissent en soi un outil analytique puissant, et depuis longtemps utilisé par les services de renseignements. Surtout, elle néglige un impact de l'évolution technologique actuelle qui tend à gommer la distinction entre données relatives aux télécommunications et substance.

L'analyse des données de trafic associées aux télécommunications dans le territoire du Pacte de Varsovie a fait les belles heures des agences de renseignements occidentales tout au long de la Guerre froide, et a même servi durant la seconde guerre mondiale<sup>111</sup>. Même quand on ne peut pas lire des messages parce qu'ils sont encryptés, le seul fait que A communique avec B, puis que B communique avec C peut révéler bien des choses quant aux comportements ou aux intérêts de l'un ou de l'autre.

Dans le contexte de l'Internet, les données relatives au trafic s'avèrent plus éloquentes encore. Elles incluent inévitablement des informations relatives au système d'exploitation de l'ordinateur de la personne qui envoie une communication et à la présence de certains logiciels dans cet ordinateur et à d'autres caractéristiques techniques<sup>112</sup>. Dans le cadre de

<sup>110</sup> *Ibid.*, p. 13. On parle en anglais de *traffic data*.

<sup>111</sup> Les quelques pages du site web de la *National Security Agency* états-unienne relatives à l'impact de l'analyse des télécommunications dans le cadre de la bataille de Midway, en 1942, comportent d'ailleurs certaines indications à cet égard: la source paraît au moins à cet égard inattaquable. Ce site évoque également le même type d'activités dans le cadre de la guerre de Corée.

<sup>112</sup> Pour s'en convaincre, le lecteur est incité à consulter la page «Vos traces...» de la Commission nationale informatique et libertés, au [www.cnil.fr/traces/index.htm](http://www.cnil.fr/traces/index.htm), ainsi que le site <http://privacy.net/analyze>. Il pourrait apprendre bien des choses sur sa propre connexion Internet... et sur ce que peuvent savoir de lui les exploitants de tous les sites web qu'il visite, ainsi que toute entité qui n'intercepterait que les données de trafic.



l'usage d'un engin de recherche, elles incluent aussi des indications relatives à la nature de la recherche effectuée. Posons par exemple qu'un cinéphile qu'a passionné le film «Bagdad Café»<sup>113</sup> et qui, curieux d'en savoir plus, utilise un engin comme Google pour naviguer en recherchant sous les mots: *Bagdad, desert et sidewinder*<sup>114</sup>. L'adresse web de la page de références générée par Google et expédiée<sup>115</sup> à ce cinéphile sera la suivante:

[www.google.ca/search?q=bagdad+desert+sidewinder&ie=UTF-8&oe=UTF-8&hl=en&meta=](http://www.google.ca/search?q=bagdad+desert+sidewinder&ie=UTF-8&oe=UTF-8&hl=en&meta=).

Voilà des données de trafic bien bavardes, et qui attireraient assurément l'attention de policiers préoccupés par le terrorisme, alors qu'on a pourtant affaire à un cinéphile tout à fait inoffensif (mais qui ne suit sans doute pas l'actualité d'assez près...).

Là encore, on peut multiplier les exemples. Songeons au citoyen qui apprend qu'un ami homosexuel est séropositif. L'usage qu'il fera d'un engin de recherche sur le web pour en savoir plus à l'égard de cette affliction et des ressources sociosanitaires disponibles dans sa région s'accompagnera de l'échange de données de trafic également stigmatisantes, et dont ce citoyen ne s'attend sans doute pas qu'elles pourraient être consultées par les autorités en l'absence de motifs raisonnables de croire qu'il pourrait être relié à la commission d'une infraction criminelle.

Il paraît donc manifeste que la distinction entre données relatives au trafic et contenu s'estompe. Rien ne permet de croire que cette tendance se résorbera. Il serait par conséquent périlleux de présumer qu'on devrait à l'avenir tolérer une attente de protection de la vie privée moins élevée à l'égard de ces données qu'à celui des contenus proprement dits, car ce serait cristalliser maintenant une règle trop complaisante à l'égard de pratiques dont l'effet sera de plus en plus délétère sur les droits fondamentaux.

Si, dans le cadre du réseau téléphonique, on a en effet historiquement tenu que l'attente raisonnable de protection de la vie privée à l'égard de ces données était relativement peu élevée, c'est que la technologie du début du vingtième siècle faisait en sorte que toutes les

<sup>113</sup> de Percy Aldon, un film réalisé en 1988, tourné en Californie et qui raconte l'histoire d'une femme qui, arrivant dans un petit café situé dans un bled perdu au milieu du désert, redonne presque miraculeusement sa vitalité à l'établissement.

<sup>114</sup> Le *sidewinder* est une sous-espèce de crotale assez abondante dans le désert de Mojave, où a été tourné le film; c'est aussi le nom que portait à l'époque l'établissement où il a été tourné. Mais c'est également le nom d'un missile air-air utilisé par les forces armées états-uniennes, notamment, ce que le cinéphile moyen pourrait ne pas savoir. L'auteur a bel et bien effectué cette recherche informatique, et n'a jusqu'à maintenant pas été inquiété par le SCRS...

<sup>115</sup> et il s'agit par conséquent de données de trafic; le lecteur s'en convaincra s'il reprend cet énoncé, l'insère dans la barre d'adressage de son fureteur et appuie sur la touche d'entrée: il s'agit d'une adresse web tout à fait valide et fonctionnelle.

communications étaient établies par une standardiste et que les lignes téléphoniques réservées à un abonné demeuraient rares. La technologie permet maintenant d'assurer un niveau de discrétion nettement plus élevé<sup>116</sup> et il eut été heureux que le droit progresse avec la technologie, au lieu de stagner.

L'interception des données reliées au trafic comporte aussi d'autres risques, apparents en matière de courriel. Il est fréquent qu'un citoyen envoie un même courriel à plusieurs personnes, en copie conforme; il est hélas presque aussi fréquent que certains des récipiendaires renverront à leur tour ce message à d'autres destinataires, sans avoir élagué la première liste de cibles. À l'égard de ce second envoi, toutes les adresses des destinataires du premier courriel sont-elles encore des données relatives au trafic, qui pourraient être interceptées?

La question relève à la fois de la technologie et du droit, et il conviendra à tout le moins de définir la notion de «données relatives aux télécommunications» pour s'assurer que celles qui pourraient être interceptées et utilisées même en l'absence de motifs raisonnables de croire à la commission ou à l'imminence d'une infraction (si ce pouvoir devait être accordé) ne seraient que celles relatives à la communication interceptée elle-même, et non aussi celles relatives aux échanges en amont ou envoyées à des tiers<sup>117</sup>. On créerait autrement des situations où une personne qui n'a absolument rien à se reprocher verrait sa vie privée examinée parce qu'un tiers qu'elle ne connaît pas, mais qui se trouvait sur une même liste de copies qu'elle, se trouve pour sa part en relation avec des éléments criminels.

En définitive, nous éprouvons des réticences à voir se généraliser des outils policiers tels que les ordonnances spécifiques de production qui sont envisagées. Ce n'est pas parce qu'elles existent déjà dans certains domaines qu'elles sont légitimes. On n'a pas rapporté la preuve que l'exigence que les autorités démontrent qu'elles ont des motifs raisonnables de croire à la commission ou à l'imminence d'une infraction réduirait significativement l'efficacité de l'action policière: après tout, les autorités doivent bien avoir une raison quelconque pour s'intéresser aux communications d'un citoyen, et ils devraient pouvoir s'en expliquer auprès d'un magistrat.

<sup>116</sup> auquel les Canadiens s'attendent et auquel les tribunaux ont déjà fait écho: par exemple, *Glover c. Bell Canada*, *op. cit.*

<sup>117</sup> qui sont aussi, au sens strict, des données relatives à une télécommunication, même si ce n'est pas à celle qui a été interceptée.

Notons aussi que la participation aux activités d'un gang ou d'un groupe terroriste constitue maintenant un crime au Canada<sup>118</sup>; il suffirait que les autorités aient des motifs raisonnables de croire qu'une personne appartient à une telle organisation pour pouvoir être autorisées judiciairement à effectuer des interceptions, en application de critères d'évaluation judiciaire qui permettent d'éviter des intrusions étatiques superflues.

Plus généralement, la teneur du Document de consultation nous paraît troublante en ce qu'on semble vouloir multiplier les types d'ordonnances que pourraient obtenir les autorités, et assortir chacun de ces types de modalités particulières. Nous n'avons pas vu de démonstration que cela contribuerait à renforcer l'efficacité du droit, ou qu'on ne pourrait pas subsumer ces divers instruments en un seul type d'ordonnance, auquel seraient associées des garanties procédurales élevées. C'est autrement miner progressivement toute attente raisonnable de protection de la vie privée au Canada.

#### **Recommandation 4**

**Nous recommandons que ne soit pas établi en droit canadien le pouvoir d'obtenir des ordonnances spécifiques de production visant les données relatives aux télécommunications en vertu de critères moins exigeants que ceux applicables à l'interception des contenus.**

#### **Recommandation 5**

**Nous recommandons que la législation précise les modalités et la portée que peut avoir une ordonnance de production visant les données de trafic relatives à des courriels.**

#### **4- les ordonnances d'obtention de données**

Il était apparemment d'usage, selon le Document de consultation, que les fournisseurs de services téléphoniques acceptent de divulguer certaines données de base à l'égard d'un client aux autorités étatiques, même en l'absence d'une autorisation judiciaire<sup>119</sup>. Notons d'abord que le fondement juridique de ces pratiques traditionnelles nous paraît un rien aléatoire, surtout depuis l'entrée en vigueur de la LPRPDÉ, dont l'alinéa 7 (3) (c.1) ne crée pas de droit nouveau à l'obtention de renseignements et ne justifierait donc pas des pratiques qui, si courantes qu'elles aient été, n'en étaient peut-être pas pour autant

<sup>118</sup> *Code criminel*, art. 83.18 et 467, la notion de «participation» étant par ailleurs définie en termes fort inclusifs.

<sup>119</sup> Document de consultation, *op. cit.*, p. 14.

légal<sup>120</sup> et ne le seraient plus en vertu des articles 4 et 5 de la LPRPDÉ et du paragraphe 4.3 de son Annexe 1.

On voudrait maintenant établir plus clairement le pouvoir des autorités d'obtenir de telles données, afin de pouvoir contraindre tous les fournisseurs de services de télécommunications à fournir de telles données même en l'absence d'un mandat. On note également que les autorités doivent maintenant composer avec les effets de certaines décisions du Conseil de la radiodiffusion et des télécommunications canadiennes qui encadrent la divulgation de l'identité d'un fournisseur de services locaux, de sorte que policiers et autres Argus pourraient désormais éprouver un peu plus de peine à déterminer qui est par exemple le fournisseur de service de téléphonie cellulaire auquel a recours un citoyen dont ils veulent surveiller les activités<sup>121</sup>.

Il nous paraît préférable que les autorités obtiennent de tels renseignements en vertu d'une ordonnance judiciaire, plutôt qu'en vertu de connivences aléatoires et furtives entre enquêteurs et fournisseurs de service de télécommunications. L'émission de cette ordonnance devrait là encore requérir que les autorités aient des motifs de croire à la commission d'une infraction.

La situation est manifestement différente lorsque les corps policiers cherchent à obtenir certaines informations dans le cadre d'une situation d'urgence ou parce qu'ils recherchent les proches de la victime d'un accident ou d'un crime, par exemple. La LPRPDÉ permet toutefois aux fournisseurs de services de communiquer certains renseignements à ces autorités dans de telles circonstances. On ne voit donc pas pourquoi, dans le cadre d'une enquête pouvant mener à des accusations contre une personne, on devrait retenir un critère moins exigeant que l'existence de motifs raisonnables de croire à la commission ou l'imminence d'une infraction pour obtenir des renseignements.

Le Document de consultation soulève d'autre part l'hypothèse qu'on pourrait à l'avenir exiger législativement des fournisseurs de service qu'ils conservent des renseignements qu'ils ne conservent pas présentement à leurs propres fins. Ce serait faire à ces entreprises l'obligation d'être en mesure d'agir comme délateurs au besoin. Ce serait requérir de leur part la conservation de renseignements qui ne sont pas nécessaires à leurs fins, et donc les

<sup>120</sup> et on a notamment à l'esprit ici la logique des tribunaux d'appel dans l'affaire *Glover*, *op. cit.*

<sup>121</sup> Document de consultation, *loc. cit.* On serait tenté d'indiquer à l'égard de ce dernier argument que l'État canadien a fait son lit quant à la déréglementation des services de télécommunication locaux au Canada et qu'il ne lui reste qu'à en assumer les conséquences, si embêtantes fussent-elles pour certaines de ses composantes.

contraindre à enfreindre la LPRPDÉ. Ce serait leur faire encourir des coûts qui ne leur paraissent pas opportuns, pour servir les policiers. Ce serait faire primer la surveillance préventive et systémique de toute la population sur la protection de la vie privée des citoyens. Ce serait inacceptable.

#### **Recommandation 6**

**Nous recommandons que l'obtention de données sur un abonné ou son fournisseur de services aux fins d'une enquête visant cet abonné et effectuée par les services policiers ou les autorités chargées de la sécurité nationale requière l'obtention d'une ordonnance judiciaire.**

#### **Recommandation 7**

**Nous recommandons que ne soit pas constituée une obligation légale faite aux fournisseurs de recueillir à l'avenir certains renseignements qu'ils ne jugent pas opportun de recueillir aux fins de la gestion de leur entreprise.**

#### 5- les ordonnances d'assistance

On fait dans le Document de consultation un parallèle entre les ordonnances d'assistance qui peuvent être accordées en vertu de l'article 487.02 du *Code criminel* et les situations où d'autres ordonnances d'interception pourraient être accordées, sans qu'il soit expressément précisé qu'elles peuvent aussi être assorties d'ordonnances d'assistance<sup>122</sup>. On voudrait que ces autres ordonnances d'interception puissent également donner lieu à des ordonnances requérant des personnes de prêter leur assistance aux autorités qui veulent effectuer l'interception.

L'accessoire suit le principal et il paraît logique que des autorités étatiques ayant obtenu un mandat judiciaire d'interception puissent le mettre en oeuvre, et donc qu'elles puissent au besoin obtenir d'autres personnes la collaboration nécessaire. Il faut toutefois prendre garde au respect des principes les plus élémentaires de justice naturelle. On peut croire en effet que ces ordonnances d'assistance sont présentement rendues sans que la personne visée ait été entendue. Or il se peut qu'elle ait des motifs juridiquement légitimes d'exprimer des réserves quant à l'effet qu'aurait sur elle une ordonnance d'assistance.

Les tribunaux ne rendent généralement de décisions *ex parte* qu'à titre intérimaire, lorsqu'une question sérieuse est en jeu<sup>123</sup>, qu'il y a manifestement risque que soit causé un

<sup>122</sup> Document de consultation, *op. cit.*, p. 15.

<sup>123</sup> *Turbo Resources Ltd. c. Petro Canada Inc.*, (1989) 24 C.P.R. (3d) 1 (C.A. fédérale).

préjudice irréparable<sup>124</sup> et qu'il y a urgence. Sauf dans ces cas, la procédure *ex parte* est en droit canadien une mesure exceptionnelle.

On ne compte en effet dans les lois canadiennes qu'une centaine de cas où la loi autorise expressément un tribunal à rendre une décision *ex parte* et les principes de justice naturelle s'opposent à ce qu'une ordonnance soit rendue à l'encontre d'une personne sans qu'elle en ait été informée<sup>125</sup> et sans qu'elle ait pu faire valoir ses arguments<sup>126</sup>. Il s'agit dans la quasi-totalité des cas prévus dans la législation de situations où la nature même de l'affaire soumise au tribunal rend impossible la présence de l'autre partie. On songe notamment ici aux dispositions relatives à l'émission d'un mandat de perquisition ou de mandats semblables, dans la mesure où on exclut du débat la personne dont on veut justement intercepter les communications à son insu<sup>127</sup>.

L'audition *ex parte* est également permise dans des cas où des impératifs de protection de la sécurité nationale font en sorte que le gouvernement veut empêcher que des éléments de preuve soient communiqués à des personnes<sup>128</sup>; là encore, ce n'est pas le cas de figure qui nous intéresse. D'autres cas relèvent par leur nature de l'injonction provisoire<sup>129</sup>. Quelques dispositions gouvernent également l'accès à des éléments de

<sup>124</sup> *Cutter (Canada) Ltd. c. Baxter Travenol Laboratories of Canada Ltd.*, (1980) 47 C.P.R. (2d) 53 (C.A. fédérale), requête pour autorisation de pourvoi à la Cour suprême rejetée (1980) 47 C.P.R. (2d) 53n (C.S.C.); *Apotex Inc. c. Imperial Chemical Industries plc*, [1990] 1 C.F. 221 (C.A. fédérale).

<sup>125</sup> *Lapointe c. Association de bienfaisance et de retraite de la police de Montréal*, [1906] A.C. 535 (C.P.); *Moshos c. Ministère de la Main-d'oeuvre et de l'Immigration*, [1969] R.C.S. 886; *Confederation Broadcasting (Ottawa) Ltd. c. C.R.T.C.*, [1971] R.C.S. 906, 924-925; *Costello et Dickhoff c. Ville de Calgary*, [1983] 1 R.C.S. 14; *Cardinal c. Kent*, [1985] 2 R.C.S. 643, 655; *Supermarchés Jean Labrecque c. Flamand*, [1987] 2 R.C.S. 219; *S.E.P.Q.A. c. Canada (C.C.D.P.)*, [1989] 2 R.C.S. 879, par exemple.

<sup>126</sup> *Komo Construction Inc. c. C.R.T.Q.*, [1968] R.C.S. 172; *Singh et al. c. Ministère de l'Emploi et de l'Immigration*, [1985] 1 R.C.S. 178; *S.I.T.B.A. c. Consolidated-Bathurst Packaging Ltd.*, [1990] 1 R.C.S. 282; *Board of Education of the Indian Head School c. Knight*, [1990] 1 R.C.S. 653, notamment.

<sup>127</sup> On pense par exemple à l'alinéa 26 (3) de la *Loi sur les ressources en eau du Canada*, L.R.C. 1985, c. C-11, ou à l'article 185 du *Code criminel*, L.R.C. 1985, c. C-46, relatif aux autorisations d'écoute électronique; près des deux tiers des cas d'utilisation de la notion d'*ex parte* dans la législation fédérale relèvent de l'émission de mandats.

<sup>128</sup> Ces cas sont rares et bien circonscrits, et on peut y jumeler les cas relatifs aux questions de défense et de relations internationales: on pense notamment aux articles 47 et 52 de la *Loi sur l'accès à l'information*, L.R.C. 1985, c. A-1 (la portée de ce dernier ayant toutefois été jugée excessive par la Cour suprême dans l'arrêt *Ruby*, *op. cit.*), aux articles 38 ss. de la *Loi sur la preuve au Canada*, L.R.C. 1985, c. C-5, à l'alinéa 103.1 (7) de la *Loi sur l'immigration*, L.R.C. 1985, c. I-2, ou aux articles 46 et 51 de la *Loi sur la protection des renseignements personnels*, L.R.C. 1985, c. P-21.

<sup>129</sup> Par exemple, l'article 34 de la *Loi sur la concurrence*, L.R.C. 1985, c. C-34.

preuve particulièrement délicats, comme des documents couverts par le secret professionnel de l'avocat<sup>130</sup>. Ces cas particuliers sont décrits en détail dans la législation pertinente. De manière générale, les quelques cas où le pouvoir de procéder *ex parte* a été accordé indiquent qu'il s'agit d'une mesure d'exception, à laquelle on ne devrait avoir recours que lorsque la chose est inévitable<sup>131</sup>.

Si on devait étendre la faculté des autorités étatiques d'obtenir de telles ordonnances, il faudrait donc à tout le moins y greffer un mécanisme permettant à la personne visée de demander au juge qui l'a rendue (ou, au besoin, à un autre magistrat) de la réviser pour des motifs de droit ou pour cause d'impossibilité en fait de s'y conformer, par exemple. Ce mécanisme de contrôle devrait être léger et rapide, et on peut croire qu'il ne serait invoqué qu'assez exceptionnellement, mais il paraît nécessaire pour protéger les droits de la personne visée par l'ordonnance d'assistance.

Il va d'autre part de soi que de telles ordonnances devraient préciser l'identité de leur destinataire et fournir certains paramètres quant à la nature de l'assistance qui est requise de leur part.

#### **Recommandation 8**

**Nous recommandons qu'il soit envisagé d'étendre la portée des ordonnances d'assistance qui peuvent être émises, à condition notamment qu'elles soient assorties d'un mécanisme de révision à la demande de la personne visée et de précisions relatives à leur portée.**

#### **6- les ordonnances de conservation**

Au motif notamment que les États qui ratifieront la Convention sur la cybercriminalité devraient en vertu de ses dispositions<sup>132</sup> constituer dans leur droit national un instrument procédural de cette nature, le Document de consultation propose l'établissement en droit canadien d'ordonnances de conservation, qui obligeraient le fournisseur de services à l'adresse de qui elles sont émises à stocker pendant une période donnée les données qu'il traite ou détient à l'endroit d'une personne déterminée<sup>133</sup>. Plus précisément,

<sup>130</sup> Par exemple, les alinéas 462.48 (13) et 488.1 (9) du *Code criminel*, L.R.C. 1985, c. C-46 et l'alinéa 293 (14) de la *Loi sur la taxe d'accise*, L.R.C. 1985, c. E-15.

<sup>131</sup> Tout devrait néanmoins être mis en oeuvre pour que les principes de justice naturelle soient appliqués dans toute la mesure du possible: *Durayappah v. Fernando*, [1967] 2 A.C. 337 (C.P.).

<sup>132</sup> et notamment de son Article 16.

<sup>133</sup> Document de consultation, *op. cit.*, pp. 15-17.

Il s'agit d'une ordonnance judiciaire qui exige du fournisseur de services visé qu'il stocke et conserve toutes les données existantes qui se rapportent à une transaction ou à un client spécifique. Il s'agit d'une mesure temporaire qui serait en vigueur seulement pour la durée nécessaire afin de permettre à l'organisme d'application de la loi d'obtenir un mandat l'autorisant à saisir les données ou une ordonnance de production des données.<sup>134</sup>

Il faut noter que la création d'un tel mécanisme comporte certaines difficultés, et même certains périls.

Les fournisseurs de service (et il s'agit toujours de déterminer la portée de cette notion) devront en effet régler des problèmes pratiques qui peuvent s'avérer substantiels. Il faut envisager deux (2) cas de figure, également embêtants pour des raisons fort différentes.

Dans le premier cas, le fournisseur n'a pas pour pratique de conserver beaucoup de données à l'égard des opérations traitées dans son réseau. Il expurge quotidiennement ses registres de transactions, par exemple. Il se trouverait donc pratiquement incapable de se conformer à une ordonnance de conservation, à moins de modifier peut-être significativement ses pratiques d'exploitation. Cela peut s'avérer coûteux et compliqué, et ne pourra peut-être pas être réalisé en temps utile<sup>135</sup>. Il se peut par contre que des traces presque imperceptibles des opérations passées puissent encore être extraites de ces systèmes et on sait que des techniques informatiques sophistiquées permettent de déceler sur des supports mémoriels des documents en principe effacés complètement. Pour se conformer à une ordonnance de conservation, un fournisseur pourrait-il être obligé de se soumettre à de telles vérifications de ses registres et des supports qu'il possède?

Dans le second cas, le fournisseur a pour habitude de conserver une quantité appréciable de données relatives aux opérations effectuées sur son réseau<sup>136</sup>. Si ces opérations ont quelque importance, la masse de données stockée pourrait s'avérer fort considérable. Se pose alors potentiellement la problématique du repérage exhaustif de celles de ces données qui sont relatives à la cible visée par l'ordonnance de conservation,

<sup>134</sup> *Ibid.*, p. 15.

<sup>135</sup> car les modifications requises à ses systèmes informatiques pourraient prendre quelques heures ou quelques jours, pendant lesquels ne seront pas préservés des éléments visés par l'ordonnance et qui pourraient être d'un grand intérêt pour les autorités.

<sup>136</sup> ce qui pose en soi des problèmes juridiques liés à la conformité aux lois relatives à la protection des renseignements personnels, mais c'est une autre affaire.



opération pour laquelle les systèmes du fournisseur ne sont peut-être pas parfaitement configurés. Là encore, des coûts appréciables pourraient devoir être encourus, sans qu'on sache dans quelle mesure les fournisseurs en seront dédommagés par l'État.

La situation sera d'autant plus compliquée pour le fournisseur qu'on lui demanderait de conserver toutes les données qu'il détient à l'égard d'une personne qui n'est pas son abonné. Un fournisseur de service de téléphonie cellulaire devrait alors tenter de repérer tous les cas où le (514) 598-7288 a tenté de rejoindre un de ses propres clients, par exemple; il se peut qu'une telle recherche ne soit pas précisément facile à effectuer. Rien, dans le libellé du Document de consultation, ne s'oppose à une telle extension de l'effet d'une ordonnance à toutes les données qui pourraient concerner une transaction spécifique. On veut bien croire que telle n'est pas la volonté des auteurs du Document de consultation, mais il conviendrait de fournir plus de précisions à cet égard, d'autant que le libellé de l'Article 16 de la Convention n'exclut pas non plus qu'on donne une telle portée à une ordonnance de conservation.

En somme, la création d'un mécanisme tel que les ordonnances de conservation pourrait fort bien constituer pour les fournisseurs qui veulent restreindre leur risque juridique et administratif un incitatif à stocker plus de données sur leurs clients et à les indexer plus efficacement. Elle favoriserait donc potentiellement l'essor de pratiques qui nuisent de manière générale à la protection de la vie privée et des renseignements personnels. Il s'agit là d'un effet pervers d'une telle mesure que le législateur voudra garder à l'esprit quand il déterminera s'il doit aller de l'avant à l'égard de la mise en place d'une telle procédure. C'est, là encore, institutionnaliser pernicieusement la surveillance.

Il faudra d'autre part établir plus clairement la portée temporelle que pourrait avoir une ordonnance de conservation. Vise-t-elle simplement à interdire au fournisseur de détruire les données constituées après son émission, ou vise-t-elle également toutes les informations que détient ce fournisseur à l'égard de la cible visée, y compris celles déjà stockées au moment de l'émission de l'ordonnance? Dans le second cas, il faudrait à tout le moins préciser le registre temporel que vise l'ordonnance, pour ne pas obliger un fournisseur à se plonger dans les copies papier de registres constitués il y a dix ans et qui seraient encore conservées dans un centre d'archivage quelconque.

Plus fondamentalement, la raison d'être même d'une procédure comme l'ordonnance de conservation paraît nébuleuse. D'abord, il s'agit ici encore de multiplier les procédures. Ensuite, le Document de consultation lui-même reconnaît que l'émission d'une telle

ordonnance requerrait normalement une décision judiciaire<sup>137</sup>; mais pourquoi, alors, ne pas obtenir immédiatement un mandat de perquisition ou une ordonnance de production assortie d'une ordonnance d'assistance?

Nous éprouvons donc des réserves importantes à l'égard de l'ordonnance de conservation, qui peut aussi donner lieu à des abus. Le Document de consultation évoque l'hypothèse qu'elles puissent demeurer en vigueur pour des périodes allant de quatre-vingt-dix (90) à cent quatre-vingts (180) jours<sup>138</sup>; pourraient-elles au surplus être renouvelées? Avec quel degré de précision définira-t-on le champ visé par une ordonnance? Pourrait-elle viser, par exemple, toutes les communications concernant une entreprise donnée? Selon la taille de l'entreprise visée, cela pourrait constituer une quantité importante de données et requérir la conservation de renseignements concernant des tiers qui ne sont en aucune manière visés par l'enquête en raison de laquelle l'ordonnance a été émise. Bref, il faudra s'assurer que le recours aux ordonnances de conservation ne glissera pas insensiblement vers l'implantation de pratiques qui ressembleraient à s'y méprendre à du stockage préventif de données.

#### **Recommandation 9**

**Compte tenu des informations présentement disponibles, nous recommandons que ne soit pas établi en droit canadien le pouvoir d'obtenir des ordonnances de conservation.**

#### **7- la propagation des virus**

L'adhésion à la Convention sur la cybercriminalité requerrait que certaines précisions soient apportées en ce qui a trait aux infractions existant en droit canadien en matière de propagation de virus informatiques ou de certains dispositifs illégaux<sup>139</sup>. On ne voit pas là de difficulté de principe; on ne pourra toutefois juger de l'impact d'éventuelles modifications législatives que lorsqu'on pourra en examiner le libellé.

<sup>137</sup> Document de consultation, *op. cit.*, p. 16, où on propose la création d'une exception afin que des ordonnances non judiciaires puissent être émises dans des «circonstances extraordinaires». Outre qu'on voit mal ce qu'elles pourraient être, c'est admettre que les ordonnances émises dans des circonstances «ordinaires» le seront par un juge.

<sup>138</sup> et cela étonne d'autant plus que le par. 16 (2) de la Convention ne requiert la conservation des données que durant une période de 90 jours; on ne voit pour quelle raison la loi canadienne devrait exiger davantage.

<sup>139</sup> En vertu notamment de l'Article 6 de la Convention.

Nous notons par ailleurs que le Document de consultation demeure muet à l'égard de la reconnaissance en droit canadien d'autres types d'infractions, et notamment de ceux visés à l'Article 3 de la Convention en matière de prohibition des interceptions de transmission d'informations. Certes, les dispositions du *Code criminel* en matière d'interception embrassent une bonne part des comportements qu'il s'agirait effectivement d'interdire (et on entend également préciser le statut du courriel, comme on le verra dans la prochaine section). Nous invitons toutefois le gouvernement à s'assurer que le droit existant permet bel et bien de sanctionner toute interception non légalement autorisée, y compris lorsqu'elle est le fait d'un agent de la Couronne ou d'un agent de la paix.

#### **Recommandation 10**

**Nous recommandons que puissent être précisées en droit canadien la nature et la portée des infractions relatives à l'usage de virus informatiques ou d'autres procédés d'altération de données, à condition notamment que le statut des infractions relatives à l'interception de télécommunications soit également précisé.**

#### **8- l'interception du courriel**

Le Document de consultation n'est nulle part plus précis à l'égard de sa description d'une problématique que lorsqu'il décrit les difficultés conceptuelles associées à la détermination de la nature du courriel et aux questions soulevées par son interception<sup>140</sup>. Il faut savoir gré aux auteurs de cette section d'avoir tenté de baliser plus précisément la discussion. Nous admettons avec eux qu'il convient de préciser le statut du courriel et qu'il convient que son interception soit pour l'essentiel assujettie à des exigences similaires à celles posées par la partie VI du *Code criminel*.

Le Document de consultation signale toutefois l'existence de trois (3) situations où l'analyse serait plus délicate: les cas de stockage du courriel chez le fournisseur de l'expéditeur; ceux de stockage chez le fournisseur du destinataire, et ceux de conservation d'un courriel ouvert chez le fournisseur du destinataire. Nous estimons que, dans tous ces cas, les courriels ne devraient pouvoir être obtenus par les autorités qu'en vertu d'un mandat ou d'une ordonnance judiciaire émis à cette fin, sous la forme d'une interception ou d'une saisie. Cela paraît la solution préconisée dans le Document de consultation à l'égard des deux (2) premières situations notées; elle s'impose également dans le dernier cas.

<sup>140</sup> Document de consultation, *op. cit.*, pp. 17-19.

Les auteurs du Document de consultation errent en effet dans leur description de la situation résultant du maintien par le fournisseur de services d'une copie d'un courriel ouvert par le destinataire, qu'ils décrivent dans les termes suivants:

Cette situation ressemble au cas d'une personne qui, après avoir lu une lettre, la dépose dans un classeur plutôt de la jeter à la poubelle.<sup>141</sup>

Avec respect, cela ne correspond pas à la réalité. L'internaute qui, ayant lu un courriel qu'il a reçu, le jette, le rend nettement moins repérable sur son ordinateur<sup>142</sup>. Il n'a toutefois aucune espèce de contrôle informatique sur ce que fait son fournisseur de services à l'égard d'une copie de ce courriel qu'il aurait conservée dans ses fichiers. Si le fournisseur conserve une telle copie, l'internaute ne peut la détruire lui-même; tout au plus pourrait-il user de recours d'ordre juridique pour réclamer du fournisseur qu'il supprime le document, en vertu des règles relatives à la gestion des renseignements personnels. Nous posons toutefois l'hypothèse que la plupart des internautes ignorent que bien des fournisseurs de services conservent en mémoire, pendant un certain temps au moins, des courriels que ces internautes croient avoir détruits.

L'analogie qu'il aurait été opportun de faire dans le Document aurait donc dû être la suivante: «cette situation ressemble au cas d'une personne qui, après avoir lu une lettre, la jette à la poubelle sans savoir que le facteur en conserve la photocopie qu'il a faite avant de lui livrer cette missive». Cela change quelque peu l'analyse. Il ne s'agit plus de présumer que le citoyen consent à ce que subsiste une copie du document<sup>143</sup>, mais de postuler qu'il le croit détruit. L'attente raisonnable en matière de protection de la vie privée dans les circonstances paraît donc foncièrement différente. Elle sera faible dans le premier cas, et nettement plus considérable dans le second.

Les règles relatives à la consultation d'une copie d'un courriel détenue par le fournisseur de services après que le destinataire en ait pris connaissance, et ce à l'insu du destinataire ou sans qu'il puisse détruire cette copie, devraient donc être aussi rigoureuses

<sup>141</sup> *Ibid.*, p. 18.

<sup>142</sup> On sait en effet qu'il ne le détruit pas, et que des techniques informatiques permettent le plus souvent de reconstituer intégralement un document «jeté». La mise à la poubelle a généralement pour seul résultat d'altérer une partie de l'adresse informatique du document et d'informer le système d'exploitation que l'espace qu'il occupe peut au besoin être réutilisé à d'autres fins.

<sup>143</sup> L'analogie effectuée dans le Document vaut dans les cas où l'internaute classe le courriel qu'il a reçu dans un fichier sur son propre ordinateur à des fins de conservation, ce qui est évidemment une toute autre chose.

que celles qui s'appliquent à l'interception de ces courriels. Rien ne paraît justifier une autre solution.

Le Document de consultation n'aborde par ailleurs pas une autre question qui paraît pourtant importante. On sait qu'une communication téléphonique peut être interceptée, même sans mandat, avec le consentement de l'une des parties à l'appel. Cela se conçoit: la participation à un appel constitue un geste actif, les autres participants sont normalement au fait de la présence de chacun d'eux et l'un ou l'autre peut en tout temps s'en retirer. Il s'agit d'établir si, de la même manière, un courriel peut être intercepté ou saisi par les autorités en l'absence de mandat, grâce au consentement de l'une des parties.

Le consentement de l'expéditeur pourrait fort bien avoir ce résultat. Le consentement du destinataire le pourrait sans doute aussi, à condition toutefois qu'il s'agisse d'une enquête visant l'expéditeur. En effet, il paraît *a priori* illégitime d'opposer à un co-destinataire un consentement à l'interception d'un message qu'il reçoit et qui serait fourni par un autre co-destinataire dont la cible ignore peut-être l'existence, et à la participation duquel elle n'a pas pu consentir. Le destinataire, passif, et qui fait office de cible d'une enquête se trouve dès lors en quelque sorte piégé dans un échange auquel participe une personne en qui il n'a peut-être aucune confiance, ce qui diffère nettement de la situation où un tiers participe à une conversation téléphonique dont la cible peut à tout moment se retirer. Le risque n'étant pas le même, l'ampleur du consentement tacite à une interception consentie par un participant à la communication doit aussi différer. Il s'agit d'une nuance qui méritera plus ample réflexion de la part des parlementaires afin de maintenir un régime d'interception et de saisie équilibré au Canada.

Il paraît par conséquent opportun que le statut du courriel soit précisé en droit canadien, en exigeant dans tous les cas qu'il ne puisse être intercepté ou saisi par les autorités étatiques que lorsque l'expéditeur ou le destinataire principal y a consenti ou qu'elles ont obtenu un mandat judiciaire justifié par des motifs raisonnables de croire qu'une infraction a été commise ou pourrait l'être. Il paraît nettement préférable qu'un régime juridique unique soit créé à l'égard de ces communications, qui pourra s'appliquer tant à l'interception qu'à la saisie.

#### **Recommandation 11**

**Nous recommandons que soit précisé le statut du courriel en droit canadien à l'égard des règles relatives à son interception ou sa saisie et que le régime mis en place soit analogue à celui visant l'interception des communications téléphoniques.**

## 9- les modifications à la *Loi sur la concurrence*

Le Document de consultation accorde par ailleurs une attention particulière à certaines difficultés auxquelles le Bureau de la concurrence fait face dans la réalisation de sa mission visant à lutter contre les pratiques commerciales frauduleuses. Il va de soi que nous sommes particulièrement sensibles à l'importance de cette mission. Nous ne savons également que trop que les commerçants frauduleux déploient de l'imagination et, parfois, des moyens importants pour parvenir à leurs fins. Le défi que doit relever le Bureau de la concurrence paraît donc effectivement considérable.

Nous ne sommes cependant pas sans éprouver une certaine réticence à confier davantage de pouvoirs encore aux agents du Bureau en matière de perquisition et de fouille. Il y a en effet un certain danger à multiplier les organismes dotés de pouvoirs policiers, sans qu'on soit assuré par exemple que les agents du Bureau détiennent la formation requise et alors qu'ils ne sont vraisemblablement assujettis à aucun processus de contrôle déontologique. Lorsque le Bureau doit procéder à des opérations comme des perquisitions, on est tenté de se demander pour quelle raison il ne pourrait obtenir la collaboration des corps policiers locaux ou de la Gendarmerie Royale du Canada pour l'assister dans de telles occasions.

Par ailleurs, les «autres» pouvoirs d'ordonnance dont on aimerait doter le Bureau sont décrits si brièvement, et dans des termes si vagues, sans qu'on ait encore là rapporté la preuve de leur nécessité, qu'on aurait grand-peine à conclure qu'une démonstration convaincante qu'il devait effectivement être doté des pouvoirs évoqués.

### **Recommandation 12**

**Compte tenu des informations disponibles, nous recommandons que les pouvoirs de perquisition et de fouille accordés au Bureau de la concurrence ne soient pas étendus à ce stade.**

## 10- d'autres modifications législatives

Le Document de consultation aborde enfin<sup>144</sup> une problématique qu'on a évoquée précédemment et qui a trait à l'obtention par les autorités de renseignements relatifs à l'identité du fournisseur d'un service donné. La question se pose en effet dans les termes suivants, surtout (pour l'instant) en matière de téléphonie cellulaire: qui est le fournisseur

<sup>144</sup> *op. cit.*, p. 20.

à qui est rattaché l'abonné utilisant un numéro donné? En pratique, les services policiers peuvent difficilement l'établir, et donc savoir à qui s'adresser pour intercepter les communications de cet abonné, par exemple.

Comme l'indique le Document de consultation, le CRTC a dans une large mesure clarifié les règles à cet égard dans une décision rendue plus tôt en 2002. Nous ne croyons pas utile d'ajouter à cette décision. Il nous paraît cependant primordial que, quoi qu'ait plaidé Bell Canada dans le cadre de cette instance mue devant le CRTC, l'identité du fournisseur de services locaux d'un abonné donné constitue bel et bien un renseignement personnel relatif à cet abonné, puisqu'il s'agit d'une information qui peut être reliée à un individu identifiable.

On revient également à la charge dans le Document de consultation à l'égard de la constitution aux fournisseurs d'obligations de conservation et de production de renseignements, même dans les cas où ces entreprises ne conservent actuellement pas ces données. Pour les motifs que nous avons exposés *supra*, nous ne pouvons qu'être en profond désaccord à l'égard de telles mesures, comme à l'égard de la constitution de fichiers nationaux.

En somme, et ici encore, on n'a en rien fait la preuve que des mécanismes extraordinaires, attentatoires aux droits fondamentaux et ayant des conséquences sur l'ensemble de la population canadienne, devraient être mis en place pour faciliter le travail policier.

### **Recommandation 13**

**Compte tenu des informations disponibles, nous recommandons que ne soient pas mises en place des mesures particulières relatives à l'identification des fournisseurs de services, outre celles qu'a déjà adoptées le CRTC.**

Abordons enfin une dernière question. Il suffit de parcourir la Convention sur la cybercriminalité pour saisir qu'elle a constitué une source d'inspiration à l'égard des mesures législatives envisagées et décrites dans le Document de consultation. Ce dernier n'aborde toutefois pas d'autres aspects de cette Convention, et notamment ceux relatifs à la collaboration avec les autorités d'autres États. Nous n'en ferons donc pas ici un relevé exhaustif. Qu'il suffise de dire que, comme plusieurs des mesures que nous avons examinées *supra*, ces obligations que ferait la Convention au gouvernement du Canada s'il la ratifiait nous inquiètent aux plans de la protection de la vie privée et d'autres droits

fondamentaux des Canadiens et de la préservation de la souveraineté nationale. Il nous paraît par conséquent prématuré, sinon injustifié, que le Canada ratifie cette Convention.

**Recommandation 14**

**Nous recommandons instamment que le Canada ne ratifie pas la Convention sur la cybercriminalité du Conseil de l'Europe.**

It is seldom that liberty of any kind is lost  
all at once.

David Hume (1711-1776)



## **Recommandations**

### **Première recommandation**

Nous recommandons que les propositions contenues dans le Document de consultation fassent l'objet d'une vaste consultation publique, soutenue par la publication de toutes les informations qui y sont nécessaires et portant sur l'ensemble de la problématique, et qu'aucune de ces propositions ne soit mise en oeuvre avant que cette consultation soit terminée.

### **Recommandation 2**

Nous recommandons instamment qu'on n'établisse pas en droit canadien une obligation aux fournisseurs de service de garantir la capacité d'interception de toutes les télécommunications et que, si une telle obligation devait malgré tout être constituée, elle soit très rigoureusement balisée, notamment au plan des modalités, du partage des coûts, des circonstances dans lesquelles l'État peut en tirer parti et de la divulgation de son impact à toute la population.

### **Recommandation 3**

Compte tenu des informations présentement disponibles, nous recommandons que ne soit pas établi en droit canadien le pouvoir d'obtenir des ordonnances générales de production.

### **Recommandation 4**

Nous recommandons que ne soit pas établi en droit canadien le pouvoir d'obtenir des ordonnances spécifiques de production visant les données relatives aux télécommunications en vertu de critères moins exigeants que ceux applicables à l'interception des contenus.

### **Recommandation 5**

Nous recommandons que la législation précise les modalités et la portée que peut avoir une ordonnance de production visant les données de trafic relatives à des courriels.

### **Recommandation 6**

Nous recommandons que l'obtention de données sur un abonné ou son fournisseur de services aux fins d'une enquête visant cet abonné et effectuée par les services policiers ou les autorités chargées de la sécurité nationale requière l'obtention d'une ordonnance judiciaire.

#### **Recommandation 7**

Nous recommandons que ne soit pas constituée une obligation légale faite aux fournisseurs de recueillir à l'avenir certains renseignements qu'ils ne jugent pas opportun de recueillir aux fins de la gestion de leur entreprise.

#### **Recommandation 8**

Nous recommandons qu'il soit envisagé d'étendre la portée des ordonnances d'assistance qui peuvent être émises, à condition notamment qu'elles soient assorties d'un mécanisme de révision à la demande de la personne visée et de précisions relatives à leur portée.

#### **Recommandation 9**

Compte tenu des informations présentement disponibles, nous recommandons que ne soit pas établi en droit canadien le pouvoir d'obtenir des ordonnances de conservation.

#### **Recommandation 10**

Nous recommandons que puissent être précisées en droit canadien la nature et la portée des infractions relatives à l'usage de virus informatiques ou d'autres procédés d'altération de données, à condition notamment que le statut des infractions relatives à l'interception de télécommunications soit également précisé.

#### **Recommandation 11**

Nous recommandons que soit précisé le statut du courriel en droit canadien à l'égard des règles relatives à son interception ou sa saisie et que le régime mis en place soit analogue à celui visant l'interception des communications téléphoniques.

#### **Recommandation 12**

Compte tenu des informations disponibles, nous recommandons que les pouvoirs de perquisition et de fouille accordés au Bureau de la concurrence ne soient pas étendus à ce stade.

#### **Recommandation 13**

Compte tenu des informations disponibles, nous recommandons que ne soient pas mises en place des mesures particulières relatives à l'identification des fournisseurs de services, outre celles qu'a déjà adoptées le CRTC.

#### **Recommandation 14**

Nous recommandons instamment que le Canada ne ratifie pas la Convention sur la cybercriminalité du Conseil de l'Europe.



December 16, 2002

**BY E-MAIL and REGULAR MAIL**

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, Ontario K1A 0H8

Re: Lawful Access Consultation Document – Released by the Department of  
Justice, Industry Canada and Solicitor General Canada on August 25, 2002

To whom it may concern,

We wish to inform you that Microcell Telecommunications Inc. ("Microcell") has received a copy of today's submission by the Canadian Wireless Telecommunications Association ("CWTA") on the above-noted subject, and we fully support the positions expressed therein.

We thank the Departments for the opportunity to comment on this matter, and remain,

s.19(1)

Yours very truly,



Microcell Telecommunications Inc.

/des

cc:  CWTA

Telephone (514) 937-2121  
Fax (514) 937-2554

Suite 400  
Montreal, Quebec  
H3B 4W8 Canada

Microcell Telecommunications Inc.  
1250 René-Lévesque Blvd. West

OFFICE OF THE  
CHIEF OF POLICE



TEL: (705) 264-1201  
FAX: (705) 267-6198  
EMERGENCY: 911

## TIMMINS POLICE SERVICE

150 ALGONQUIN BOULEVARD EAST  
TIMMINS, ONTARIO  
P4N 1A7

16 December 2002

Justice Canada  
Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8

Dear Minister Cauchon:

### Re: Lawful Access Consultation Document Response

Please consider this an official and final response from Timmins Police Service with respect to the "Lawful Access" consultation process that ends on December 16, 2002.

We have had the opportunity to review the submissions made by the Canadian Association of Chiefs of Police (CACP). The Timmins Police Service agrees and supports the submission in whole.

Sincerely,



s.19(1)

CHIEF OF POLICE  
Timmins Police Service

c.c. Honourable Wayne Easter  
Solicitor General of Canada

Honourable Allan Rock  
Minister of Industry

000512



BY FAX

December 16, 2002

Hon. Martin Cauchon  
Minister of Justice and Attorney General of Canada  
284 Wellington Street  
Ottawa, Ontario K1A 0H8

Hon. Wayne Easter  
Solicitor General of Canada  
340 Laurier Avenue West  
Ottawa, Ontario K1A 0P8

Hon. Allan Rock  
Minister of Industry  
235 Queen Street  
Ottawa, Ontario K1A 0H5

**Comments on *Lawful Access – Consultation Document* (August 25, 2002) – OIPC  
File No. 16763**

This letter comments on the above consultation document of the Department of Justice, Industry Canada and the Solicitor General of Canada. That document invites comments on legislative proposals for lawful access by law enforcement agencies to communications and related information.

## 1.0 SUMMARY

- No evidence has been offered that existing interception and search and seizure laws are inadequate for dealing with electronic communications. Nor does the Cyber-Crime Convention offer a persuasive rationale for the proposals.
- Privacy is a constitutionally protected right. Privacy in electronic communications should give way to law enforcement and national security needs only where those needs clearly outweigh the privacy interest and then only to the minimal extent necessary. There is clearly a reasonable expectation of privacy in e-mail. Existing standards respecting interception of private communications should apply to e-mail interception.

---

Mailing Address: PO Box 9038, Stn Prov Govt, Victoria B.C. V8W 9A4  
Location: Fourth Floor, 1675 Douglas Street  
Telephone: (250) 387-5629 Facsimile: (250) 387-1696  
Toll Free enquiries through *Enquiry BC* at (800) 663-7867 or (604) 660-2421 (Vancouver)  
website: <http://www.oipc.bc.ca>

- Requiring service providers to acquire the technical capacity to provide lawful access inappropriately co-opts the private sector in state surveillance. The costs to service providers will raise consumer costs and may diminish the competitiveness of the Canadian Internet industry, thus exacerbating concerns about private sector involvement in state surveillance. The development and implementation of Internet technology will be driven by the interests of surveillance and not the needs or realities of Canadian businesses and consumers.
- A specific production order for telecommunications associated data should be available only from a judicial authority applying existing standards and not lower thresholds. Production orders for subscriber or service provider information also should only be available from a judicial authority applying existing standards.
- A data preservation order should be available only from a judicial authority using existing interception standards. Law enforcement authorities should, consistent with s. 487.11 of the *Criminal Code*, only be able to secure preservation when it would be impracticable to obtain a judicial order in the circumstances.
- In the context of creation of a number of surveillance databases in Canada, the proposal of the Canadian Association of Chiefs of Police to create a mandatory-reporting database of all subscribers is worrisome. Final comment is withheld, however, pending further clarification of the proposal and its details.
- Independent oversight of the nature and frequency of use of any new lawful access powers is necessary, recognizing that such oversight must be designed to appropriately protect law enforcement interests.

## 2.0 DISCUSSION

2.1 Where is the Evidence of Need? – The consultation document says that, for law enforcement and national security agencies, lawful access is an essential tool in the prevention, investigation and prosecution of serious offences and the investigation of security threats. It says telecommunications and computer networks such as the Internet can be used “in the planning, coordination, financing and perpetration of crimes and threats to public safety and the national security of Canada” (p. 3). The paper also says, at p. 3, that

... rapidly evolving technologies pose a significant challenge to law enforcement and national security agencies that require lawful access to communications and information, as these technologies can make it more difficult to gather the information required to carry out effective investigations.

The paper contends that, in light of the easy flow of information and communications around the world, law enforcement and national security agencies “need modern and effective capabilities to support their investigative or intelligence gathering efforts” (p. 4). For this reason, the document suggests “partnerships with Canadian industry are more important than ever and must be consistently fostered and maintained” (p. 4).

It is striking that the consultation document offers no evidence to support any suggestion that law enforcement or national security activities have been, or could reasonably be expected to be, impaired because existing laws respecting interception or search and seizure are inadequate given present technologies or trends in communication technologies or information flows. In the absence of any persuasive case, based on concrete evidence, that existing Canadian law is inadequate, I question the need for new laws. I am deeply concerned that – bearing in mind that the lawful access proposals are in various respects rather vague at this stage – the proposals weaken existing legal protections for privacy in Canada without a clear and compelling justification.

The contention that changes in Canadian law are necessary so Canada can ratify the Council of Europe *Convention on Cyber-Crime* ("Cyber-Crime Convention") only goes so far. That treaty is encountering very serious resistance, notably in Europe, because of the serious concerns it raises about individual liberty and privacy and because of concerns about the costs to the private sector of implementing treaty-conformed national laws.

In Australia, for example, the Senate has rejected the *Telecommunications Interception Legislation Amendment Act 2002*. In South Africa, the *Interception and Monitoring Act* was abandoned because of public resistance. In recent weeks, officials of the Home Office in the United Kingdom have conceded that the government must begin again with its implementation of the interception and seizure aspects of the much-criticized *Regulation of Investigatory Powers Act*. Among the few countries to have succeeded in enacting laws or implementing proposals comparable to aspects of the Canadian proposals are China, Iraq and Saudi Arabia.

The Government of Canada should only proceed further with the lawful access proposals if a clear evidentiary basis is offered to support the need for changes. To be sure, the Government of Canada should not proceed simply because it is expedient to do so in the post-September 11 climate of fear and insecurity.

Bearing this overriding reservation in mind, the balance of this letter comments on specific aspects of the proposals assuming, only for the purposes of argument, that a need for them has been established on clear evidence.

**2.2 Privacy and Electronic Communications** – I will first note the constitutional dimensions of privacy in communications and address privacy in e-mail communications.

#### *Privacy and the Canadian constitution*

The constitutional dimensions of the right to privacy are beyond debate. The Supreme Court of Canada has on many occasions affirmed that the *Canadian Charter of Rights and Freedoms* affords constitutional protection for Canadians' privacy. For present purposes, I need only quote from the Court's decision in *R. v. Duarte*, [1990] 1 S.C.R. 30, at paras. 21 & 22, which relates to interception of communications:

The rationale for regulating the power of the state to record communications that their originator expects will not be intercepted by anyone other than the person intended by the originator to receive it (see definition section of Part IV.1 of the

[*Criminal Code*] has nothing to do with protecting individuals from the threat that their interlocutors will divulge communications that are meant to be private. No set of laws could immunize us from that risk. Rather, the regulation of electronic surveillance protects us from a risk of a different order, *i.e.*, not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.

The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States v. White, supra* [401 U.S. 745 (1971)], put it, at p. 756: "Electronic surveillance is the greatest leveller of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.

In debate over anti-terrorist and other measures, I have consistently acknowledged that law enforcement agencies and national security agencies should not be hampered in their law enforcement and national security activities by unwarranted concern for individual privacy rights. The balance between state interest and individual rights should only favour state interests, however, where a law or other measure has been shown to be clearly necessary and to intrude on individual privacy only to the least extent practicable. The existing *Criminal Code* provisions respecting interception of private communications appropriately balance individual privacy interests against the public interest in effective law enforcement.

#### *E-mails are private communications*

The consultation paper appears to suggest that e-mails are not private communications. It refers to s. 183 of the *Criminal Code*, which defines "private communication" as including any telecommunication or oral communication made under circumstances creating a reasonable expectation of privacy. The paper suggests that this indicates that a written communication is not a "private communication". The paper refers to decisions by some courts that tape-recorded messages, like written letters, are not "private communications" within the meaning of the *Criminal Code* definition, because it is not reasonable for anyone sending a tape or letter to expect that it will remain completely private.

The consultation paper's appeal to the existing *Criminal Code* definition of "private communication", and to court decisions dealing with it, does not advance the analysis. The question remains, should e-mails be regarded as private communications? The obvious and only answer is that e-mails are private communications. The fact that it may be possible for hackers or others to intercept an e-mail using inappropriate technologies or methods does not undercut this. Surely all Canadians regard letters they send to be



private despite the risk that someone will steal them from a mailbox and improperly read them? Such a risk may influence what information is included in private correspondence, but prudence in protecting sensitive information does not mean the correspondence is not a private communication.

The Alberta Court of Appeal has held that there is a reasonable expectation of privacy in e-mail. See *R. v. Weir*, [2001] A.J. 869 (affirming [1998] A.J. No. 155). As the trial judge noted in that case, in *United States v. Maxwell*, [1995] 42 M.J. 568, the U.S. Air Force Court of Criminal Appeals held, at p. 576, that e-mails carry an objective expectation of privacy, in the following terms:

However, we find appellant definitely maintained an objective expectation of privacy in any e-mail transmissions he made so long as they were stored in the America Online computers

In our view, the appellant clearly had an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords. Unlike transmissions by cordless telephones, or calls made to a telephone with six extensions, or telephone calls which may be answered by anyone at the other end of the line, there was virtually no risk that the appellant's computer transmissions would be received by anyone other than the intended recipients.

An e-mail should be explicitly recognized by our criminal law as a private communication and should be protected accordingly. Existing *Criminal Code* interception standards should apply and lower standards for interception of e-mails are not desirable. Many of the weaknesses of consultation paper proposals stem from the apparent assumption that e-mail is not a private communication and does not deserve protection as such. Other flaws in the proposals flow from the similar assumption in the paper that data associated with e-mail traffic, Internet addresses and traffic and other such data do not engage privacy interests because they have little or no privacy content.

**2.3 Imposing Lawful Access Capabilities** – The consultation document suggests that all wireless, wireline and Internet service providers should be required to ensure that their systems have the technical capacity to provide lawful access to law enforcement and national security agencies. This intercept capability would include content and 'telecommunications associated data' (as the latter term is defined in the document).

The proposal to require Internet service providers to meet certain technical standards amounts to forcing businesses to collect and organize data in a manner that is driven by the need to provide lawful access – in the interests of alleged law enforcement needs and state surveillance – rather than a particular business imperative. This could skew business models and the market, not to mention the impact on consumers.

First, I echo the serious concern voiced around the world that imposition of this capability on service providers inappropriately conscripts the private sector as an agent of the state, not a partner, who engages in surveillance for the state. This point is fundamental. Imposition of a technical intercept capability would greatly blur the line

between surveillance activities of, or on behalf of, the state and commercial surveillance. Creation of a surveillance state is, of course, to be avoided at all costs, but that is precisely the direction in which this proposal tends.

Second, such a proposal carries grave cost implications for service providers, especially Internet service providers. The bursting of the Internet bubble may have set back electronic commerce, but it did not destroy it. Imposition of a costly lawful access capacity requirement will almost certainly further inhibit electronic commerce. Have such risks and benefits of imposing such a lawful access requirement been assessed? In the Netherlands, for example, cost implications for Internet service providers have been so significant that the government has been forced several times to postpone the deadline for compliance with a technical intercept capacity requirement legislated a few years ago. Similar concerns have been expressed, and difficulties encountered, in the United States under the 1996 *Communications Assistance to Law Enforcement Act*. European Union countries have encountered stiff resistance from service providers on this very issue.

While these cost implications do not directly affect privacy interests, I am concerned that the end-result could be to cause consolidation in the Internet service industry. Such a consolidation would reduce competition, could affect service levels and certainly would exacerbate concerns about private sector surveillance on behalf of the state. Moreover, this proposal would amount to state policy regarding law enforcement and surveillance driving development and application of technology, not the market.

**2.4 Production Orders** – The consultation document indicates that several types of production orders are being considered for enactment: a general production order, a specific production order for traffic data and a specific production order for subscriber or service provider information (or both). By production order, the document means an order that would compel service providers to produce information to law enforcement agents within a set period.

As I understand it, a general production order would be similar to a search warrant, the salient difference being that a production order would require the service provider to deliver documents to a law enforcement agency or make them available to that agency. In the case of a search warrant, of course, law enforcement agents enter relevant premises to find and take away all material covered by the warrant.

The following comments focus on the proposed specific production orders. At the very least, in each instance I believe that existing legal standards must be preserved. No case has been made for lower standards. As regards the paper's reference to "anticipatory orders", the concept is not fleshed out, so I cannot comment.

#### *Specific production orders for telecommunications associated data*

The consultation document proposes, at p. 11, that a specific production order should be available "under a lower standard" than existing *Criminal Code* thresholds for telecommunications associated data, supposedly because Internet traffic data is comparable to telephone number records and dial-number recorders.

I strongly disagree with the paper's assumption that there is a lower expectation of privacy in relation to Internet traffic data, comparable to telephone number-related records and dial-number recorder data. The proposed definition of telecommunications associated data would, in the context of e-mail and Internet use, appear to enable law enforcement agents to obtain the following data: e-mail sent-to and received-by addresses; computer IP addresses; data respecting duration of communications; data as to date and time of communications; data about the size of a communication; data disclosing websites visited; and, possibly, data as to e-mail subject line and attachment file names.

By contrast, dial-number recorders merely record identifying information about telephone numbers called from a specific telephone number, not call-content information or other potentially sensitive information of the kinds I have just described. Further, in the case of wireless telephones, which would be covered by the lawful access proposals, unit location information would be in issue, this distinguishing such data from dial-number recorder data.

The reality is that telecommunications associated data can yield a rich lode of information using data-mining and other techniques to disclose information about the intimate details of Canadians' personal lives. Any analogy between dial-number recorders and telecommunications associated data should be rejected and specific production orders for such data should only be available applying existing *Criminal Code* standards. I also note that, before enactment of s. 492.2 of the *Criminal Code*, the Ontario Court of Appeal ruled that use of dial-number recorders to obtain local call information without prior judicial authorization contravened the *Criminal Code* prohibition against interception of private communications. See *R. v. Griffith* (1988), 44 C.C.C. (3d) 63. Canadian courts were not unanimous in this view, but the fact remains that the Ontario Court of Appeal and other courts across the country considered even dial-number recorders to be problematic in the absence of any legislated protections for privacy.

The document also proposes, rather obscurely, that a specific production order should be available under a lower standard for unspecified "other data or information in relation to which there is a lower expectation of privacy" (p. 12). It is not possible to comment usefully on this proposal in the absence of better information as to what is intended.

#### ***Production order for subscriber and service provider information***

The consultation paper notes that law enforcement authorities must get "some form of court order" to obtain subscriber or service provider information where that information is not voluntarily disclosed to them by its custodian. The paper also acknowledges that basic customer information has traditionally been made available to law enforcement officials. Yet it is suggested that a specific production order could be made available even if no investigation is under way and according to an unspecified lower threshold.

I am concerned that the case for such orders has, again, not been made out. If law enforcement agencies have traditionally been able to get such information it is not clear to me why authority to compel it is needed. Certainly, if custodians have historically delivered such information to law enforcement agencies to assist existing investigations,

I have reservations about allowing compelled disclosure in non-investigative situations. I am, therefore, skeptical about the need for this proposal, at the very least, and would want to see more detail before commenting further.

**2.5 Data Preservation Orders** – As the consultation document indicates, the Cyber-Crime Convention contemplates a new tool, called a preservation order. Such orders require service providers to retain and preserve data for as long as it takes a law enforcement agency to obtain a warrant to seize the data or a production order requiring its delivery to the agency.

I am not opposed in principle to this proposal. I accept that, because of the nature of electronic data, it may be necessary for law enforcement agencies, in limited cases, to be able to obtain a preservation order to give them time to apply for a warrant or production order from the appropriate judicial authority. The standards to be applied in obtaining such an order from a judicial authority should ideally be comparable to existing standards. The standard of reasonable grounds to believe an offence has been or may be committed may be one approach to examine.

This is not to say that I support the breadth of the proposals found in Articles 16 and 17 of the Cyber-Crime Convention. To the contrary, I believe those articles are excessively broad. I am also concerned that the 90, 120 or 180-day retention periods mentioned in the consultation paper are excessive. If any preservation order provision is enacted, it should apply only to stored computer data (not paper records), it should be available only in the context of an ongoing investigation into a possible violation of a criminal law and preferably should be available only from a judicial authority applying the criteria of reasonable grounds.

As regards exigent circumstances, where not even a preservation order pending warrant can be obtained, law enforcement authorities should at most be empowered to require a service provider to preserve information only where, consistent with s. 487.11 of the *Criminal Code*, obtaining a judicially-issued preservation order "would be impracticable" in the particular circumstances. It is worth underscoring here my concern that no evidence has been presented whatsoever that this or any of the other proposals is needed because existing laws are inadequate.

The fine line between data preservation orders and legislated data retention requirements must be acknowledged. The latter concept is even more troubling, of course, since it entails creation of massive surveillance databases. For example, in the United Kingdom a one-year retention period for data has been imposed. Apart from the civil liberties concerns data retention raises, one wonders about its efficiency or efficacy. The cost implications are enormous. In a December 12, 2002, ZDNet article, America Online is reported as estimating, in testimony before an all-party Parliamentary inquiry in the United Kingdom, that its setup costs alone to comply with United Kingdom law are roughly £30million, with the same again in running costs. That is the cost for just one Internet service provider. The cost implications of data preservation orders also cannot be underestimated, but certainly data retention requirements should be avoided at all costs.

2.6 **National Database of Subscriber Information** – I have serious reservations about the proposal of the Canadian Association of Chiefs of Police for establishment of a national database of subscriber information. In addition to the concern that this would also conscript the private sector into surveillance, the creation of such a centralized database must be viewed in light of other database proposals either under way or on the table. I refer here, as an example, to the Canada Customs and Revenue Agency's air traveller database, about which I have previously expressed grave concern.

The proliferation of such databases is deeply troubling. Now more than ever such proposals must be subjected to close scrutiny before they proceed. Failing clear evidence that a national database of subscribers is necessary because existing means of collecting subscriber information are inadequate, or that such a database would actually work and not be circumvented by criminals, I believe the proposal should not be pursued at this time. At the very least, if the proposal proceeds, concerns about accountability and independent oversight are critical and must be addressed.

2.7 **Accountability** – Nowhere does the consultation paper indicate that accountability measures are being contemplated. If new and broader powers are enacted, and I again suggest the case for them has not been made, a system of accountability is needed. This of course cannot be allowed to jeopardize law enforcement or national security interests, but independent oversight of the frequency and nature of use of new powers is necessary. A body such as the Security and Intelligence Review Committee should be considered in relation to any new law enforcement access to e-mail and other electronic communications data, bearing in mind my concern that the case for the proposed powers has not been made.

Yours sincerely,

s.19(1)

David Loukidelis  
Information and Privacy Commissioner  
for British Columbia

cc: Lawful Access Consultation  
Criminal Law Policy Section  
Department of Justice

George Radwanski  
Privacy Commissioner of Canada

Provincial & territorial privacy commissioners and ombudsmen

letters/16763-ISP.doc



## F A C S I M I L E C O V E R S H E E T

Date: December 16, 2002 OIPC No. 16763  
To: Department of Justice  
Criminal Law Policy Section  
Fax Number: (613) 941-9310 s.19(1)  
From: [REDACTED] for David Loukidelis

### Comments:

Please see the attached comments on *Lawful Access -- Consultation Document*.

Number of Pages (including cover sheet): 10

The attached material is intended for the use of the individual or institution to which this fax is addressed and may not be distributed, copied or disclosed to unauthorized persons. This material may contain confidential, privileged or personal information which may be subject to the provisions of the

*Freedom of Information and Protection of Privacy Act.*

If you receive this transmission in error please notify us immediately by telephone at (250) 387-5629, or toll free through (604) 660-2421 (Vancouver) or (800) 663-7867 (elsewhere in BC).

Thank you for your cooperation and assistance.

**Pierlot, Paul**

---

From: [REDACTED]  
Sent: 2002 Dec 16 2:40 PM  
To: la-al@justice.gc.ca  
Subject: ITAC submission - lawful access

s.19(1)



lawful-access - 2002

1216.doc... Lawful Access Consultation,  
Criminal Law Policy Section  
5(superscript: th) Floor  
284 Wellington St.

Ottawa, Ontario, Canada,  
K1A 0H8

Attached is ITAC's submission. Please feel free to contact me should you wish to discuss any of these points.

[REDACTED]  
Executive Director, Policy and Planning  
Information Technology Association of Canada (ITAC)  
tel (905) 602-8510 [REDACTED]  
[REDACTED]

(See attached file: lawful access - 2002 12 16.doc)



INFORMATION TECHNOLOGY  
ASSOCIATION OF CANADA



ASSOCIATION CANADIENNE DE LA  
TECHNOLOGIE DE L'INFORMATION

## **Lawful Access**

### **ITAC Comments on *Lawful-Access Consultation Document***

**December 2002**

---

2800 Skymark Avenue, Suite 402, Mississauga, Ontario L4W 5A6 Tel: (905) 602-8345 Fax: (905) 602-8346 <http://www.itac.ca>  
2800 avenue Skymark, bureau 402, Mississauga (Ontario) L4W 5A6 Tél : (905) 602-8345 Télécopieur : (905) 602-8346 <http://www.itac.ca>



The Information Technology Association of Canada (ITAC) recognises that the federal government, having committed Canada to ratifying the Council of Europe *Convention on Cyber-Crime*, needs to amend Canada's *Criminal Code* to include provision for production orders, preservation orders and offences in relation to computer viruses that are not yet deployed. However, ITAC would not want to see measures implemented that would impose an unrealistic burden on Canadian industry or that would encroach unduly on the individual rights that contribute to the strength and attractiveness of our society.

Having reviewed the *Lawful Access Consultation Document* (August 25, 2002), ITAC is pleased to note that the government has attempted to find a sustainable balance among the needs to protect public safety, sensitive information transmitted over public networks, individual rights and the economic interests of Canadians and Canadian companies. Nevertheless, we remain concerned about several aspects of what appears to be the government's intended direction. As we have noted previously, experts have suggested that Canada's security and law-enforcement agencies do not need new powers so much as they need additional resources.<sup>1</sup>

## 1. CONSTRAINTS ON INNOVATION

One general concern is that the proposals in the *Consultation Document* tend to constrain the use of technology to meet the surveillance desires of law-enforcement and national-security agencies. Law enforcement currently must rely on its ability to take advantage of existing characteristics of technologies in use. In contrast, the proposals would require companies to install technologies with specific characteristics (i.e., that "provide at a minimum a basic intercept capability"). This appears to limit innovation, whereas the government's *Innovation Strategy* urges Canadians to strive to promote new and innovative services.

In addition, legislation or regulation that would increase the regulatory burden, or introduce other costs to be borne by service providers, would likely delay the introduction of new products and services that connect Canadians and help people embrace the knowledge economy. Time and resources that service providers might have devoted to research and development will now have to go to upgrading software, hardware, etc. Additional burdens may even serve to drive Canada's many small service providers out of business, again to the detriment of competition and innovation.

<sup>1</sup> ITAC letter to Minister Manley re: Cyber Security, October 24, 2001.

## **2. INTERCEPT CAPABILITY**

### **2.1 Encryption**

The *Consultation Document* proposes that service providers be required to "have the technical capability to provide access to the entirety of a specific telecommunication transmitted over their facilities". Where service providers provide the encryption, they will be required to provide intercepted communications in their decrypted form. ITAC recommends that service providers be allowed to choose either to disclose means of decryption or to provide access to the unencrypted plain text.

The use of end-to-end encryption may make it very difficult, if not impossible, for service providers to identify the specific data packets that comprise a digital communication. Furthermore, recognising that the people that police investigations target may well use strong end-to-end encryption or steganography for their messages, ITAC suggests that the preserved data will often not provide law enforcement what it is looking for.

However, ITAC is pleased to note that the government recently implemented export-control regulations dispel concerns that it would attempt to deal with this issue by re-regulating strong encryption. As is generally agreed, re-regulation would not have been in Canada's long-term interests – either as a country reliant on electronic communication or as a leading producer of encryption products and services to the international market.

### **2.2 Impact on Quality of Service**

ITAC is concerned that the basic intercept capability discussed in the *Consultation Document* may detract from the quality of service currently offered by service providers to customers with whom they may have contractual service-level obligations. We note that it will not be possible in all cases for a service provider to provide an intercept capability without impacting the quality of service to its customers or affecting the integrity of customer data.

More recent transport technologies (e.g., high-speed SONET transmission facilities, routers and switching equipment) do not lend themselves to real-time monitoring. While networking equipment has increased in capacity, intrusive monitoring devices lag behind. Therefore, in some cases transmission equipment would need to be 'slowed down' to enable real-time monitoring – thus affecting service quality and possibly causing loss of customer data. In addition, the installation of service-monitoring points within a network introduces additional potential points of failure within the architecture.

### **2.3 Regulations Relating to Intercept Capability**

ITAC looks forward to a cooperative approach, involving industry and other interested parties, to setting technical specifications to promote interoperability (domestically and internationally), apportioning costs pursuant to lawful-access legislation, and possibly discussing the ground rules for forbearance. ITAC recommends that standards developed by industry rather than regulation by government be relied upon as much as possible – and that those standards be consistent with those of our allies and trading partners. Canada cannot afford to have its regulatory and standards regimes out of synch with those of our allies.

ITAC stresses that the building-in of technologies to enable lawful access will involve not just service providers but also manufacturers of telecom equipment and computer hardware and software. If technologies with the necessary features are not available, providers will not be able to move to new services that support lawful access. Clearly all sectors of our industry need to be involved in any standards body or other industry or industry-government working group that is given the task of examining and addressing future requirements.

### **2.4 Costs of Ensuring Intercept Capability**

In ITAC's view, the application of the new provisions only to new services recognises that it is preferable to design security into a product than to attempt to retrofit it. However, it is unclear what is meant by the term "significantly upgraded service". Would it apply to service providers expanding existing services (e.g., increasing capacity or extending existing services into new geographic areas) using essentially the same hardware and software systems?

As this could be very expensive, depending on the definitions used, ITAC recommends that law enforcement be obliged to compensate service providers for their reasonable costs of providing a lawful-access capability on their networks and for carrying out lawful-access services. This would include incremental equipment or system costs associated with providing access for new or significantly enhanced services, in addition to retrofit costs for equipment and systems and operational costs for the lawful-access services used by law enforcement. In addition, service providers must be protected from liability should the equipment required to provide the necessary access be unavailable (or prohibitively expensive).

### **3. AMENDMENTS TO THE CRIMINAL CODE**

#### **3.1 Production Orders**

ITAC sees the working definition of 'telecommunications associated data' contained in the *Consultation Document* as problematic. Traffic data containing physical-location information and search terms go far beyond the simple origin, destination, time and duration information available from the current switched telephone system. In the case of voice-over-IP using IPv6, packets also identify the originating device, its physical location if wireless transmission is involved, and other data. This clearly can be "personal information that tends to reveal intimate details of his/her lifestyle and personal choices", which Parliament has specifically protected.

As noted above, one of the purposes of the proposals in the *Consultation Document* is to enable Canada to ratify the Council of Europe *Convention on Cyber-Crime*. ITAC therefore recommends that 'telecommunications associated data' be re-defined to be consistent with the narrower definition of 'traffic data' used in the *Convention* (i.e., data generated by computers in the chain of communication in order to route a communication from its origin to its destination).

#### **3.2 Preservation Orders**

ITAC believes that privacy and the protection of personal information are fundamental societal values that must not be lost as we move to protect cyberspace. While we recognise that data-preservation orders – made with judicial authority and reasonable time limits – will sometimes be necessary, it is very important that preservation orders be narrowly defined.

The preservation order presented in the *Consultation Document* would compel a service provider not to delete data that it already has in its possession. Though the order is not intended to cause service providers to store additional data, it would tend to have that effect. A preservation order would effectively apply to an entire virtual private network (VPN) since the service provider would be unable to identify individual users due to encryption. (A VPN involves, by definition, encrypted packets.) As a result, the service provider would no longer be able to release and recycle some portion of its storage capacity, a situation that would have storage-cost implications – especially for smaller service providers.

#### **3.3 Virus Dissemination**

Individuals and companies who are victims of viruses should not be in danger of being caught by a general provision regarding propagation of computer viruses. While ITAC appreciates the verbal assurances by government officials that criminal intent must exist for an offence to have occurred, we urge that legislation confirm that this is indeed the case. This is a significant issue for individual users, service providers and entities, such as software laboratories and security consultants, whose work demands that they possess viruses for legitimate testing purposes.

Some ITAC members operate as internet service providers and therefore operate servers used by subscribers for storage of their own data. ITAC recommends that a service provider not attract any liability if one of its subscribers stores a computer virus on a server without the service provider's knowledge. Nor should service providers be expected to search files stored by their clients' files to ensure that they are free of viruses.

### **3.4 Subscriber Information**

ITAC strongly objects to any obligation on service providers to collect customer name and address information that is unnecessary for service provision. By passing the *Personal Information Protection and Electronic Documents Act*, the Parliament of Canada has already answered the question, asked in the *Consultation Document*, as to whether a service provider should be compelled by law to collect such information. That act limits the collection of unnecessary personal data and the retention of personal data on file beyond the point when it might have been needed.

Furthermore, it is important to note that the imposition of a mandatory-collection rule would radically change the ways that Canadians now use prepaid wireless services and prepaid calling cards. ITAC is of the view that the implementation of lawful-access provisions should not change the way telecom services are offered or used.

## **4. PRIVACY AND PROTECTION OF PERSONAL INFORMATION**

ITAC's view is that security of data – and recourse when security is broken – must be stressed should service providers be compelled to collect subscriber information. Similarly, data captured under a preservation order, but subsequently deemed unnecessary, must be protected and ultimately destroyed so as to safeguard privacy. Not only is privacy an integral value in our society, it is a fundamental part of electronic commerce – as has been recognised by the government in its own online initiatives. ITAC recommends that lawful-access legislation be accompanied by a concerted effort to assure the public that its privacy will be protected.

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Dec 16 2:59 PM  
**To:** 'Department of Justice'  
**Subject:** CCTA's Comments on Lawful Access Consultation Document

s.19(1)



Lawful Access



CCTA Lawful Access -

Consultation.c...

Dec 16 20...

Please find attached the Canadian Cable Television Association's (CCTA's) comments on the government's Lawful Access Consultation Document.

Filing Date: December 16, 2002

<<Lawful Access Consultation - cover letter .doc>> <<CCTA Lawful Access - Dec 16 2002.doc>>

The original hard copy will follow in the mail.

[REDACTED]  
Executive Assistant, Law & Regulatory Affairs  
Canadian Cable Television Association (CCTA)  
Tel: (613) 688-5546 / Fax: (613) 232-2137  
[REDACTED]

**CANADIAN CABLE TELEVISION ASSOCIATION**  
**ASSOCIATION CANADIENNE DE TELEVISION PAR CÂBLE**

Président / Présidente

December 16, 2002

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor,  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8

Attention: The Honourable Martin Cauchon  
Minister of Justice and the Attorney General of Canada

Dear Minister:

**Re: Lawful Access Consultation**

The Canadian Cable Television Association (CCTA) hereby files its comments on the government's Lawful Access Consultation Document.

As set out in greater detail in the attached submission, CCTA has substantial concerns regarding the potential of the government's proposals to impose significant and onerous costs and obligations on service providers. CCTA is strongly of the view that no new legislative requirements should be introduced that would either restrict the ability of our members to meet their customers' reasonable expectations for privacy and security or negatively impact the rollout of innovative and advanced broadband services across Canada.

Given the absence of precision and clarity in the Consultation Document, CCTA requests that any draft legislation and accompanying regulations be made available for a full and complete public review involving all interested stakeholders. In our view, it is critical that sufficient time be provided for interested parties to assess the impact of any legislative proposals and to have a meaningful opportunity to respond and propose alternative solutions.

We thank you for the opportunity to provide these comments.

Yours truly,

s.19(1)

# **LAWFUL ACCESS CONSULTATION**

**Submission of the  
Canadian Cable Television Association**

**December 16, 2002**



*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 2 of 30*

**I. INTRODUCTION**

1. The Canadian Cable Television Association (CCTA) welcomes the opportunity to comment on the Lawful Access Consultation Document (the "Consultation Document").<sup>1</sup>
2. CCTA is the national industry association representing over 800 cable systems across Canada. Collectively, CCTA member systems deliver entertainment, information, and telecommunications services to approximately 6 million Canadian households, including more than 1.6 million subscribers to cable high-speed Internet access services.
3. As a world leader in the penetration of broadband cable modem Internet access, the Canadian cable industry has a direct and substantial interest in these proposals. Our members offer Internet subscribers a full range of Internet resources including email, real time chat, web access and web hosting, file sharing and transfers, work collaboration, virtual private networks, electronic commerce and advanced, customized internetworking applications. Cable access to the Internet is one of the leading methods for Canadians to connect to networks and perform online transactions.
4. CCTA notes at the outset that it shares the opinions of other industry members, including the Canadian Association of Internet Providers (CAIP), the Canadian Wireless Telecommunications Association (CWTA), Bell Canada and TELUS Communications Inc., that the lack of detail in the Consultation Document makes it difficult to provide meaningful comments and suggestions. Notwithstanding a number of industry meetings, including a bilateral

---

<sup>1</sup> Lawful Access Consultation Document, issued August 25, 2002 by Department of Justice, Industry Canada and Solicitor General Canada. [http://www.canada.justice.gc.ca/en/cons/la\\_al/](http://www.canada.justice.gc.ca/en/cons/la_al/).

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 3 of 30*

consultation with government officials in early October, CCTA remains unable to assess the real impact of the government's proposals.

5. In the absence of greater clarification regarding the rationale for and scope of the proposals set out in the Consultation Document, CCTA's comments are necessarily high-level. We wish to convey our substantial concern, however, about the potential of the government's proposals to impose significant and onerous obligations on service providers without sufficient regulatory or economic impact analyses. CCTA is strongly of the view that no new legislative obligations should be introduced that would either restrict the ability of telecommunications carriers and ISPs to meet their customers' reasonable expectations for privacy and security or negatively impact the rollout of innovative and advanced broadband services across Canada.
6. We support the requests of CWTA and CAIP that any draft legislation and accompanying regulations be made available for a full and complete public review involving all interested stakeholders. In our view, it is critical that sufficient time be provided for interested parties to assess the impact of any legislative proposals and to have a meaningful opportunity to submit comments.
7. In this regard, CCTA notes that law enforcement representatives have indicated their general satisfaction with the positive working relationship that they have developed with major carriers and ISPs to date. In the circumstances, CCTA submits that a "fast-track" process to introduce and implement new legislation and regulations is unwarranted and inappropriate. We strongly urge the government to ensure that any legislative or regulatory initiative is canvassed in a fair and comprehensive fashion with all interested stakeholders.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 4 of 30*

**II. SUMMARY OF CCTA COMMENTS**

8. The Consultation Document sets out four distinct sets of legislative proposals aimed at updating the existing legal framework:
- (i) Requirements for infrastructure capability
  - (ii) Amendments to the *Criminal Code*
  - (iii) Amendments to the *Competition Act*
  - (iv) Mechanisms to provide Subscriber and Service Provider information (CNA/LSPID)<sup>2</sup>
9. CCTA's questions and comments with respect to these proposals can be summarized as follows:

**Lawful access proposals should cover all service providers**

- CCTA believes that all telecommunications service providers, whether facilities-based or not, must be subject to similar lawful access requirements, except where exempted under a legitimate forbearance regime. Basic intercept capability requirements should apply to all Internet service providers (ISPs), including re-sellers and third-party providers.

**Service providers need to know what compliance means and how it will be measured**

- There is insufficient detail in the Consultation Document to allow industry members to determine whether they would be in a position to comply with the proposals and what the impact of compliance would be from a cost and operational perspective.

---

<sup>2</sup> CNA/LSPID is information pertaining to the customer name and address as well as local service provider identification.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 5 of 30*

- Any compliance criteria associated with the establishment of a basic intercept capability must be sensitive to the unique network design and architecture of different types of service providers. Technical standards should be developed in consultation with industry members.
- ISPs must be provided with clear guidelines and procedures to follow when they are in receipt of a court order, whether it be an intercept, preservation, assistance, production or seizure order, or any similar order granted under the *Competition Act*.

**Service providers should not bear the costs of deploying basic intercept capability**

- While it is difficult to assess with any certainty given the lack of specificity in the Consultation Document, it is clear that the costs of compliance could be significant in light of the complexity of installing, managing, operating and maintaining interception technology.
- Regardless of the manner in which "significant upgrade" and "new service or technology" are ultimately defined, CCTA considers that service providers should not be required to bear any of the costs of ensuring basic intercept capability until such time as appropriate technical solutions are widely available and can be deployed and maintained at no significant incremental cost to the service provider.
- Imposing intercept capability costs on service providers would discourage innovation and negatively impact the government's agenda of ensuring the rollout of advanced broadband services to all regions of the country.
- Service providers should be compensated for all reasonable costs associated with providing operational assistance to law enforcement. Compensation should not be established through a fixed schedule of

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 6 of 30*

fees but rather should continue to be negotiated on a bilateral basis between the service provider and law enforcement.

**Service provider liability should be limited through explicit safe harbour provisions**

- CCTA submits that explicit safe harbour provisions are warranted for service providers who act in good faith when complying with lawful access requests.

**CCTA is strongly opposed to the creation of any national ISP subscriber database**

- The creation and maintenance of a national ISP subscriber database is technically and economically unfeasible for service providers and raises significant privacy and security concerns.

**III. REQUIREMENT TO ENSURE INTERCEPT CAPABILITY**

**A. Who has to Comply? Creating an Appropriate Definition of Service Provider**

10. The Consultation Document sets out the following working definition of "service provider" at page 4:

"service provider" means a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada.

11. The working definition of "transmission facility" is set out at page 7:

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 7 of 30*

"transmission facility" means any wire, cable, radio, optical or other electromagnetic system, or any other (similar) technical system, used for the transmission of information between network termination points.

12. These working definitions are virtually identical to the definitions of "telecommunications common carrier" and "transmission facility" as set out in s. 2 of the Telecommunications Act<sup>3</sup>. These definitions pertain to the ownership and operation of physical network facilities used to provide telecommunications services to the public. The effect of using these definitions in the context of lawful access obligations is that the definitions would only capture facilities-based service providers that provide services to the public for compensation.
13. In CCTA's view, the current working definition is under-inclusive, creating the possibility that a significant portion of service providers will not have to provide intercept capability. This would lead to the creation of a safe haven for criminal activities, which would render the legislation meaningless and ineffective. It would also result in facilities-based service providers bearing an unfair burden.
14. Most on-line criminals conduct transactions by hacking into the accounts of others, using anonymizers or masking their identity (for example, by changing header information). Alternatively, criminals create a private web site accessible only to their group. Private web sites number in the hundreds of thousands around the globe, with little known about their owners or content. Generally, sites owned and operated by criminals are not hosted on servers at the ISP premises. Mobile servers and mobile Internet connectivity for such sites have only heightened the problem and difficulties for law enforcement. Such challenges are not solved by interception of data through a commercial ISP.

---

<sup>3</sup> *Telecommunications Act*, RSC 1993, C-38, Part 1, s. 2(1).

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 8 of 30*

15. For these reasons, CCTA considers that a more appropriate definition of service provider is that provided in the Council of Europe *Convention on Cyber-Crime*.<sup>4</sup> In the Convention, "service provider" is defined as "any public or private entity that provides to users of its service the ability to communicate by means of a computer system" and "any other entity that processes or stores computer data on behalf of such a communication service or users of such service".
16. CCTA submits that this definition would be more appropriate since it would capture all suppliers in the transmission chain (upstream access providers, resellers, application service providers, web hosting facilities), access to which could be necessary to effectively execute an order for interception, preservation, production or seizure. In addition, fairness requires that the proposed legislation regime apply equally to all classes of providers, and to all providers within a class, except in those circumstances where a service provider is legitimately forborne under any forbearance regime that might be established.

**B. What does Compliance Mean? Understanding Basic Intercept Capability**

***Definition of "basic intercept capability"***

17. The Consultation Document proposes that service providers would be required to provide, at a minimum, a basic intercept capability before providing a new or significantly upgraded service to the public. The Consultation Document does not, however, provide any definition of "basic intercept capability", nor does it specify the kind of criteria that would be considered in assessing whether a service provider is in compliance with a basic intercept requirement.

---

<sup>4</sup> Council of Europe *Convention on Cyber-Crime*, Chapter 1, Article 1(c).

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 9 of 30*

18. In the course of public consultations, government representatives attempted to provide some guidance in this regard, suggesting that the proposed legislative regime would establish detailed requirements including:<sup>5</sup>

- Real time monitoring
- Methods to correlate the intercepted data and content
- Number of simultaneous interceptions
- Interfaces, delivery methods and formats
- Service provider initiated encryption
- Quality of service
- Location information
- Physical, personnel and administrative security measures
- Access to subscriber/customer information

19. It was suggested at one of the industry consultations that the definition of "basic intercept capability" would be based on a sub-set of the above criteria. The sub-set, however, was not identified, making it almost impossible to accurately assess the impact of the government's proposal. Indeed, notwithstanding the information provided in the course of the industry consultations, the following questions remain outstanding:

- What does "basic" intercept capability mean?
- Would existing capabilities meet the standard?
- Would the definition match the requirements set out in the U.S.

*Communications Assistance for Law Enforcement Act (CALEA)*<sup>6</sup> or is something different envisioned?

---

<sup>5</sup> Presentation Slides entitled: Lawful Access Consultation, Canadian Cable Television Association – Ottawa, October 4, 2002. Department of Justice Canada, Department of the Solicitor General, Industry Canada.

<sup>6</sup> *Communications Assistance for Law Enforcement Act of 1994*, Pub. L. No. 103-414, 108 Stat. 4279. CALEA requires that telecommunications carriers have the capability to: 1) isolate expeditiously the



*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 10 of 30*

- Would equipment be certified to ensure that the minimum technical capability is met?
  - Would the criteria differ depending upon what layer in the IP Protocol stack was involved, or what Internet resource? For instance, data from a customer using Virtual Private Network software would be different than the interception of real time chat, some email client software will require different methodologies, and so forth.
  - Would equipment have to pass a reliability or performance test? Would the minimum specifications be identified? Would there be standard interface specifications? What would be the procedures for measuring/assuring on-going compliance with reliability and performance standards?
  - Would there be inspections of every service provider? What would be the qualifications of inspectors? Would inspections include all classes and types of service providers including access services and applications services?
  - Should a service provider be found lacking in one category, will there be a system of warnings and time to effect a remedy prior to imposition of a penalty? What kinds of penalties are being envisioned?
20. Assessment of compliance will be an intricate task due to the complex nature of the apparatus and procedures involved and the different technologies required depending upon system design and network configuration. CCTA requires greater clarification about the nature and scope of any proposed compliance mechanism before providing more comprehensive comments in this regard.

---

content of targeted communications transmitted by the carrier within the carrier's service area; 2) isolate expeditiously information identifying the origin and destination of targeted communications; 3) provide intercepted communications and call identifying information to law enforcement so they can be transmitted over lines or facilities leased by law enforcement to a location away from the carrier's premises; and 4) carry out intercepts unobtrusively, so targets are not made aware of the interception, and in a manner that does not compromise the privacy and security of other communications. See 47 U.S.C. 1002(a).

*Canadian Cable Television Association  
Comments on Lawful Access Consultation Document  
December 16, 2002  
Page 11 of 30*

***Technical Standards***

21. The Consultation Document suggests that technical standards and details would best be set out in regulations, the scope of which is open to discussion, but could include standards for access, security requirements and provisions for compensation. No specific proposals were made in this regard.
22. CCTA submits that technical standards should be established by persons or committees comprised of network technology experts, including industry representatives and specialists from each area of network operations. Standards should not be overly prescriptive, but should be sufficiently detailed to permit a service provider to understand its requirement under the law. Further, such standards and regulations must be determined without requiring industry members to disclose proprietary information on network architecture to competitors, industry associations or government.
23. Due to the technical nature of Internet infrastructure, any technical standards developed must be sufficiently broad and flexible to accommodate a variety of network architectures without putting any particular service provider at a competitive disadvantage. Intercept capabilities may need to be custom-developed by and for each type of service provider. These will vary from moderate to highly complex systems. Technical regulations that may be well suited to deployment in a DSL service provider may not be such a good a fit for a cable service provider. For these reasons, CCTA submits that service providers must have the flexibility to establish technical solutions that best suit their own networks. Provided that basic intercept functionality is achieved, network design should remain within the purview of service providers.
24. Some of the issues that have arisen during real time monitoring of packets include: problems with the volume of data, problems isolating the target, issues surrounding the location within the networks of the monitoring point, network

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 12 of 30*

interference and performance issues (particularly where the speed of the traffic exceeds the speed of the monitoring tool), the difficulties in scalability of some of these technologies, the ease of configuration and use, the fault tolerance capabilities and the post-event audit trail. There also may be different security requirements for storage of intercepted data, depending upon the nature of the offence, and the type of data. Finally, current intrusion detection systems, filter, and other intercept tracing and tracking tools are not standardized and are not necessarily designed to collect and protect the integrity of information suitable for use in courts.

25. CCTA notes that the cost of developing "made-in-Canada" technical solutions could be prohibitive or unnecessary. In this regard, government representatives suggested during the course of industry consultations that telecommunications equipment manufacturers would develop lawful access solutions to meet both Canadian and U.S. requirements.<sup>7</sup> It was further stated that the proposed regime would be sufficiently flexible to allow industry members to select the most cost-effective technical solutions as long as the basic criteria were met.
26. CCTA is not confident that U.S. equipment manufacturers will develop technical solutions to meet Canadian lawful access requirements unless these requirements are substantially similar to U.S. requirements. In this regard, CCTA notes that under CALEA, only telecommunications service providers who offer voice telephony services are currently subject to the requirement to ensure basic intercept capability. Recognizing the costs and technical complexities associated with Internet interceptions, the U.S. has not required ISPs to provide basic intercept capability under CALEA. Until such time as American ISPs are subject to a legislative obligation to ensure basic intercept capability, there will be little or no incentive for equipment and software

---

<sup>7</sup> *Supra* note 5.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 13 of 30*

manufacturers to develop and produce Internet intercept solutions for widespread use in the North American market.

27. CCTA submits that, ultimately, the responsibility for developing compliant equipment must rest with manufacturers (both hardware and software providers) and suggests that the law enforcement agencies should provide details of their requirements to these suppliers. Further, CCTA submits that any off-the-shelf solution purchased from the U.S. that is deemed to be compliant with legislative requirements for intercept capability in that country should be considered adequate for compliance under any Canadian regulations.

*Operational Standards*

28. It is unclear from the Consultation Document whether service providers would be subject to specific operational standards. In CCTA's view, the extent to which service providers are expected to be involved in lawful access operations needs to be clearly identified with specific demarcation points, indicating where law enforcement responsibility begins and service provider responsibility ends for any particular intercept request. During bilateral consultations, various law enforcement agencies appeared to have different procedures regarding ownership, responsibilities and demarcation points. CCTA suggests that the government establish clear guidelines to inform service providers of the precise extent of their compliance obligations.
29. For example, the Consultation Document refers to requirements relating to how intercepted information is to be handled. It is unclear if such requirements would include security clearances for service provider staff and contractors. There are obviously costs and operational issues associated with the administration of such security clearances for personnel, including ensuring that

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 14 of 30*

an employee with proper security clearance is always on duty during an intercept operation. Moreover, from a practical perspective, it may be impossible to isolate access to a particular customer's information without alerting other networking staff. The result could be that an entire IT department would have to have adequate security clearance, with potentially significant cost and resource implications.

30. Related to this issue is the suggestion in the Consultation Document that regulations could be enacted to prescribe standard requirements for the reliability of employees. Again, there is uncertainty surrounding what would constitute a reliable employee.

- Would reliability be measured by job performance or job title or job description?
- Would such classifications vary in accordance with the type of case involved (e.g., cases involving domestic crime would require a different level of reliability than those involving national security)?
- How many employees would be required to be "reliable" within a specific operation?

**C. Costs of Compliance – Who pays?**

31. Once the definition of "basic intercept capability" is established and the technical and operational criteria for compliance are determined, the question arises as to which party will be responsible for the costs of compliance. In this regard, there are two distinct types of costs to be considered, namely infrastructure costs and operational costs.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 15 of 30*

***Infrastructure costs***

32. Government representatives have assured industry members that service providers will not be responsible for the costs of retrofitting their networks to ensure basic intercept capability, on the grounds that it would be unreasonable to require service providers to assume the costs of a retrofit to an existing network. Under the government's proposal, service providers would only become responsible for these costs when they deploy new technologies or services or undertake a significant upgrade to their system. The rationale for this position appears to be that it would be more efficient and cost-effective to build intercept capability into the network at the time a service provider performs a major upgrade to the network.
33. Because there are no definitions for "basic intercept capability", "new technology", "new service" or "significant upgrade", it is virtually impossible to assess the potential magnitude of costs for industry members. It is evident, however, that these costs could be substantial and potentially onerous for service providers. CCTA notes that following the implementation of similar legislation in the United States, a study conducted by IDC<sup>8</sup> estimated that interception software built into network switching equipment (for telephony) could cost between USD \$50,000 and USD \$500,000, depending upon the size of the network and the number of switches. For the reasons set out below, the costs for Internet service providers could be much higher.
34. CCTA disagrees with the government's underlying assumption that the deployment of basic intercept capability will necessarily be more efficient or

---

<sup>8</sup> IDC Study on costs of intercept requirements for Telecom providers see:  
[http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article\\_Type1&c=Article&cid=1035773819570&call\\_page=TS\\_Business&call\\_pageid=968350072197&call\\_pagepath=Business/News&col=969048863851](http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_Type1&c=Article&cid=1035773819570&call_page=TS_Business&call_pageid=968350072197&call_pagepath=Business/News&col=969048863851).

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 16 of 30*

cost-effective merely because the service provider is upgrading its network or introducing a new service. Indeed, if the government's rationale is that it is unreasonable to require service providers to bear the costs of retrofitting their existing networks to ensure basic intercept capability, CCTA notes that for the foreseeable future, every deployment by an Internet service provider of basic intercept capability - whether in response to a request from law enforcement or at the time of performing a significant upgrade - will effectively amount to retrofit of the provider's network. Standardized solutions do not exist today nor will they exist in the near future.

35. Accordingly, regardless of the manner in which "significant upgrade" and "new service or technology" are ultimately defined, CCTA considers that service providers should not be required to bear any of the costs of ensuring basic intercept capability until such time as appropriate technical solutions are widely available and can be deployed and maintained at no significant incremental cost to the service provider. More specifically, service providers should only become responsible for the costs of deploying basic intercept capability when such capability becomes available as a standard product offering from a wide variety of equipment vendors, with no impact on scalability and performance of such equipment and at no more than a nominal cost incremental to the equipment itself.
36. CCTA notes that integration of basic intercept equipment with provisioning software will be enormously complex, as such software is often highly customized to each service provider's operational and business needs. It is unlikely that a provisioning solution deployed by one provider will easily fit into another provider's business and network infrastructures. For these reasons, service providers should not be responsible for the costs of deploying new or upgraded provisioning software in support of an intercept capability.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 17 of 30*

37. While as noted earlier it is difficult to comment meaningfully on the government's proposal without greater clarification as to the scope of definitions such as "basic intercept capability", "significant upgrade" and "new service", CCTA strongly urges the government not to impose an undue financial or administrative burden on Canadian telecommunications carriers and ISPs. Imposing intercept capability costs on service providers prior to the widespread availability of low-cost technical solutions would put Canadian ISPs at a competitive disadvantage and would discourage innovation. It would also negatively impact the government's agenda of ensuring the rollout of advanced broadband services to all regions of the country.

***Operational costs***

38. The Consultation Document seeks input on whether regulations should provide for fees to be paid to a service provider for operational assistance. CCTA strongly believes that service providers should be compensated for all reasonable costs associated with providing operational assistance, including initial outlay and installation of equipment, any costs associated with the day-to-day maintenance of equipment (including rack space, power, air conditioning, and other associated costs) and any other costs required for on-going compliance with lawful access legislation.
39. Service providers should also be able to seek compensation for costs associated with network reconfiguration, network outages, impacted performance, and troubleshooting of issues caused or exacerbated by equipment required for compliance with lawful access legislation. CCTA further submits that service providers should be compensated for any additional administrative burdens, such as personnel training and supervision, necessitated as a result of a lawful access request.



*Canadian Cable Television Association  
Comments on Lawful Access Consultation Document  
December 16, 2002  
Page 18 of 30*

40. While CCTA considers that reasonable cost recovery for lawful access services rendered by service providers is appropriate, we do not support a formal tariff or fee structure setting out fixed fees for operational assistance. Currently, cost recovery is negotiated on an individual basis between law enforcement and the service provider. This appears to be working to the satisfaction of most parties and reflects the fact that costs will vary considerably from provider to provider depending on the nature of the specific request.

***Forbearance***

41. The Consultation Document suggests that a forbearance regime may be appropriate to provide the flexibility to adapt to special situations and to avoid the creation of "intercept safe-havens". Forbearance would remove the obligation to comply with the requirements of the statute or regulations, in whole or in part, for a limited time. The Consultation Document does not make any proposals or suggestions in terms of appropriate forbearance criteria.
42. In CCTA's view, while forbearance may be warranted in cases where compliance is not technically or economically feasible, any forbearance regime must establish clear and consistent criteria to ensure that "intercept safe-havens" are not easily created and to prevent the development of competitive inequities in the telecommunications market. Moreover, any forbearance regime should not disadvantage compliant service providers relative to non-compliant providers. CCTA requires more details as to the circumstances that would justify forbearance before making any further comments or suggestions in this regard.

#### **IV. AMENDMENTS TO THE CRIMINAL CODE**

##### **A. Overview**

43. The Consultation Document proposes a number of amendments to the Criminal Code to deal with the interception and search-and-seizure of electronic data. The proposed amendments stem from concerns raised by law enforcement and national security agencies. These agencies argue that new legal processes are required in today's on-line environment to support their investigative and intelligence gathering efforts. In addition, the Consultation Document suggests that these amendments are required in order to modernize existing legal procedures to accord with the Council of Europe Convention on Cyber-Crime, a treaty that Canada has pledged to ratify. To this effect, the paper proposes sweeping amendments to the Criminal Code with respect to production orders, assistance orders, data preservation orders and intercept orders.
44. The proposals raise significant concerns and questions for CCTA members. As a general comment, CCTA reiterates its concern that the Consultation Document fails to provide the ISP industry with the clarity required to assess the scope of their obligations. In any event, whether dealing with production orders, assistance orders, data preservation orders or interception orders, we urge the Government to ensure that ISPs:
- understand the scope of their obligations when complying with judicial orders;
  - are compensated for all reasonable costs associated with the execution of these orders; and
  - are adequately protected in terms of explicit limitations on criminal and civil liability.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 20 of 30*

**B. What does compliance mean? Understanding the nature and scope of the obligations**

***Production Orders***

45. As noted by the Consultation Document, a production order requires the custodian of documents to deliver or make available the documents to persons such as law enforcement officials within a specified period. The government proposes to expand the use of production orders, enabling law enforcement to obtain certain documents or data in the possession of ISPs. In particular, the Consultation Document seeks comments on the following legislative proposals:

- the creation of a general production order, which according to the Consultation Document could be anticipatory in nature;
- the creation of a specific production order for "traffic data"; and
- the creation of a specific production order for subscriber and/or service provider information.

46. The Council of Europe Convention on Cyber-Crime outlines very specific information that ought to be available on the issuance of production orders.

This includes:

- the type of communication service used, the technical provisions taken thereto and the period of service;
- the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; and
- any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

*Canadian Cable Television Association  
Comments on Lawful Access Consultation Document  
December 16, 2002  
Page 21 of 30*

47. CCTA has significant concerns regarding the creation of these types of orders, primarily because there is insufficient information in the Consultation Document as to the scope of ISP obligations under such orders. For example:

- Under what circumstances, if any, would ISPs be required/entitled to notify a subscriber that a production order has been issued?
- What would constitute a "document" for the purposes of a production order? Would an Internet Protocol Packet be considered a document?
- At what point would a service provider become a "custodian" of a document or piece of information?
- What would be the security and confidentiality requirements of the service provider when handling information pursuant to a production order?

48. Moreover, it is unclear whether production orders would only be issued with respect to customer name and address and local service provider identification information (CNA/LSPID), or whether traffic data would also be requested. In the public consultations, the kind of information subject to production orders was described as "non-biographical core information". If traffic data is included because it is generally considered non-biographical, at what point does such data become biographical content worthy of privacy protection and therefore a search warrant? For example, certain Internet activity patterns in the aggregate could reveal personal preferences or relationships, and not just the suspected location of the targeted individual.

*Assistance orders*

49. As noted by the Consultation Document, the Criminal Code currently contains provisions that deal with the issuance of an assistance order. An assistance order will be issued concurrently with an authorization to intercept, a search warrant or an order authorizing the use of a dial number recorder when a

*Canadian Cable Television Association  
Comments on Lawful Access Consultation Document  
December 16, 2002  
Page 22 of 30*

person's assistance may reasonably be required to give effect to these orders. In the context of lawful access, government representatives have suggested that assistance orders should spell out what could specifically be required under such orders in order that service providers understand more clearly the extent of their obligations. CCTA could not agree more.

50. An assistance order should at all times spell out what is specifically required of a service provider. For example, could an assistance order theoretically include the responsibility to decrypt secure communications? This of course would be impossible where the ISP does not hold the key. Clarification in this regard would greatly assist service providers when complying with judicial orders generally.

***Data Preservation Orders***

51. Data preservation orders would require service providers to store and save existing data that is specific to a transaction or client. We understand from our consultations with various government department officials that the proposals do not contemplate a general requirement to retain data. CCTA notes that it would be strongly opposed to any data retention obligation, which in our view would create impossible network, personnel and financial obligations. For example, IDC estimates that a small ISP of 1,000 customers would require up to 30 terabytes<sup>9</sup> (30 trillion bytes) of storage to hold the data that passes through it system for six months.<sup>10</sup> Storage requirements and the consequent costs would be much greater for larger ISPs.

---

<sup>9</sup> A terabyte is used to measure capacities of high capacity data storage. It is equal to one thousand gigabytes, one million megabytes, or one trillion bytes. A byte is usually 8 binary bits of data grouped together to form a character, digit or other value. From: Webster's New World Dictionary of Computer Terms, 5<sup>th</sup> Edition. 1994.

<sup>10</sup> *Supra* note 8.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 23 of 30*

52. CCTA notes that the Consultation Document indicates that a preservation order “would require an Internet Service Provider not to delete specific existing information relating to a specific subscriber.” We assume that this indicates the government’s intent to use data preservation orders in a limited manner. In any event, CCTA considers that the legislation should contemplate some form of “reasonable limits” in terms of the volume of data to be captured, stored and delivered. The absence of such reasonable limits could lead law enforcement and the ISP industry down a slippery slope towards a general obligation to retain data. For the reasons articulated above, our members would vigorously resist such an outcome.
53. In addition, there are some outstanding questions regarding the mechanics of data preservation, which in our view require further clarification:
- Would a hard copy printout of specified information be sufficient?
  - Who would be authorized to handle data?
  - What safeguards would need to be put in place to ensure that data is handled properly?
  - What would be an appropriate mechanism to deliver this data to law enforcement officials?
54. - The Consultation Document also seeks comment on whether 90, 120 or 180 days would be considered a reasonable period to preserve data pursuant to a data preservation order. CCTA notes that even 90 days could constitute an onerous obligation depending on the nature of the request. Data located on a network is in constant flux, with content providers adding, modifying and removing content. Moreover, Article 16 of the Council of Europe *Convention on Cyber-Crime* states that Parties to the treaty “shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 24 of 30*

necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure.” Clearly, the *Convention on Cyber-Crime* views a 90-day preservation period as a maximum obligation rather than a starting point as proposed by the Consultation Document.

55. The Consultation Document also outlines that preservation orders could, under exigent circumstances, be prospective in nature (i.e. to preserve data for a certain number of days, such as 4 days). The proposal is unclear as to whether this would involve the simple storage and saving of existing data over a number of days or whether this order would also involve the isolation, filtering or interception of data. The latter scenario raises major concerns for CCTA and its members. In our view, the isolation, filtering or interception of data, even over a limited number of days, constitutes an interception and should thus be subject to the highest standards of judicial authorization.

*Interception of e-mail*

56. The *Criminal Code* currently contains a scheme for obtaining judicial authorization to intercept private communications. E-mail poses a unique problem for legislators, however, due to the variety of ways it can be communicated, stored and accessed by network users. As the Consultation Document correctly points out, the capture of the contents of an e-mail in transit could constitute an “interception” of a private communication under the *Criminal Code* whereas the acquisition of e-mails, particularly those stored at the sender’s or the recipient’s ISP, could constitute a “search and seizure”. In either case, ISPs would certainly assert that their customers are very concerned and quite vigilant about the privacy of their email.

*Canadian Cable Television Association  
Comments on Lawful Access Consultation Document  
December 16, 2002  
Page 25 of 30*

57. Regardless of what judicial method is ultimately utilized to gain access to the contents of a subscriber's e-mail, it should be made clear in the legislation where and how the interception or seizure would be undertaken. The order seeking the information should also specify the stage of the transmission involved. What law enforcement agencies expect from ISPs and what appears in the warrant are often very different. Service providers are sometimes left in a position of having to expend their own resources to ensure that warrants are legally valid.
58. For example, some warrants currently expect that the service provider will pre-filter email and process it at the ISP end, and other warrants specifically state that it should not be reconstructed. Moreover, not all e-mail systems support the concept of "opened" vs. "unopened" e-mail. This may leave service providers in a position of being unable to execute an order to seize "opened" e-mail messages, as they may be indistinguishable from "un-opened" messages.
59. CCTA further notes that the temporal nature of email means that a customer may be able to delete messages from the server after they have received them. If an ISP knows that a customer has been targeted for lawful access is there an obligation to mirror e-mail servers to ensure that the target's email is preserved prior to capture by law enforcement? Clarification in this regard would enable service providers to assess the potential for liability and to ensure that there is a fair allocation of risk.

**C. Compensation**

60. Although the Consultation Document does not propose any formal compensation regime for the cost of complying with judicial orders, CCTA must underscore that this remains an important issue for our members.



*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 26 of 30*

61. We believe that the proposed amendments to the *Criminal Code* will significantly expand the use and scope of judicial orders authorizing lawful access to data located on a service provider's network. This is particularly true with respect to the proposals that relate to production orders and data preservation orders.
62. Although service providers are prepared to continue to provide assistance to law enforcement agencies in the conduct of their investigations, we remain concerned that compliance with lawful access requests increasingly runs the risk of putting service providers at a competitive disadvantage or financial difficulty.
63. Indeed, ISPs already incur significant costs to comply with lawful access requests. Currently, the industry has negotiated informal agreements with various law enforcements agencies and CSIS to compensate ISPs for reasonable costs associated for on-going compliance with lawful access requests. These agreements are in keeping with other jurisdictions, such as the United States, which compensate Internet service providers for the operational costs of complying with the terms of a certain judicial orders.<sup>11</sup>
64. In light of the increasing costs associated with compliance to lawful access requests, it is imperative that service providers be compensated for reasonable costs associated with compliance with any judicial order.

---

<sup>11</sup> *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. § 2518(4)(e) (provision dealing with compensation for ISP who furnish the assistance necessary to accomplish the interception); *Pen and Trap Statute*, 18 USC, § 3124(c), (dealing with compensation for reasonable expenses incurred in providing facilities or technical assistance to law enforcement).

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 27 of 30*

**D. Limitations on liability – the need for explicit safe harbour provisions**

65. CCTA is very troubled by the fact that the Consultation Document does not propose or discuss provisions that would protect service providers from criminal and civil liability, otherwise known as safe harbour provisions.
66. Law enforcement agencies are increasingly requiring ISPs to take on a significant amount of responsibility when complying with the terms of a judicial order. For example, when complying with an intercept order, some ISPs are required to target, pre-filter and process a target's e-mail communication at the ISP's head-end. Production orders, by their very nature, require ISPs to gather and transmit all the documents and data covered by the order. Compliance with these orders are often technically complex, as an ISP must gather the required information all the while ensuring the proper operation of its network and the privacy of its subscribers.
67. In addition, systems typically exhibit implementation errors from time-to-time despite the good-faith efforts of the staff. How does the policy propose to deal with such technical errors? For example, what if there is an implementation error in the intercept capability that causes interception of the wrong target's data? What if surveillance targeting information is disclosed to unauthorized individuals (either internal staff at the service provider or external to the service provider)?
68. Other jurisdictions, such as the United States, provide safe harbour provisions for Internet service providers who comply with the terms of a court order, warrant or subpoena.<sup>12</sup> No such protection currently exists for Canadian service

<sup>12</sup> See *Title III*, 18 U.S.C. § 2520(d); *Pen and Trap Statute*, 18 U.S.C. § 3124(d); *Electronic Communications Privacy Act*, 18 U.S.C. § 2703(e). See also the *U.S. Communications Decency Act of 1996* at s. 230, which provides immunity from liability for ISPs when acting in compliance and removing obscene materials from servers, as agents of the State, upon notice from law enforcement.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 28 of 30*

providers when they provide access to user's personal information or corporate records, preserve data, remove illegal content upon lawful notice, or provide assistance to law enforcement.

69. While some government officials have suggested this matter is sufficiently dealt with in section 25 of the *Criminal Code*<sup>13</sup>, CCTA is not persuaded that section 25 adequately addresses both the criminal and civil liability of ISPs in all circumstances. Meanwhile the costs for ISPs of responding to civil litigation are increasing dramatically along with the frequency of class action suits. These costs are substantial and are rising exponentially.
70. Accordingly, CCTA submits that explicit safe harbour provisions are warranted, limiting the criminal and civil liability of ISPs who act in good faith to comply with lawful access requests.

**V NATIONAL ISP REGISTRY**

71. The Consultation Document seeks comments on the appropriateness of developing a national database of subscriber information for ISPs. CCTA strongly opposes the creation of any kind of ISP subscriber registry and notes that the costs associated with developing and maintaining such a registry are almost unsurpassable.
72. We believe that the creation and maintenance of a national ISP subscriber database is technically and economically unfeasible for service providers. First and foremost, customer information is transient in nature and because it is supplied by users to the ISPs it may be flawed or out of date. Most ISPs automate their billing and obtain direct payment on customer credit cards. ISPs

---

<sup>13</sup> *Criminal Code*, R.S.C. 1985 c. C-46.

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 29 of 30*

also frequently use e-mail as the communications method with customers about billing. As such, information such as a street address may have changed since the account was set up. Consequently, such as database would inevitably suffer from major inaccuracies.

73. Second, the rationale behind the proposed national subscriber registry may be viewed as suspect by the customers of CCTA members, and those of other service providers. The purpose or usefulness of any such database is questionable, as the profile of a cyber criminal is generally someone capable of using false names, hacked accounts or public access terminals to communicate or transact.
74. The notion of registering subscriber information in a national database clearly raises significant privacy and security concerns. This would undoubtedly have a chilling affect on the use of a registered ISP, driving some customers to anonymous systems.

## **VI CONCLUSION**

75. CCTA reiterates its concern that the lack of clarity and specificity in the Consultation Document makes it virtually impossible to assess the impact of the government's proposals. Accordingly, we strongly urge the government to ensure that any draft legislation and regulations benefit from the full scrutiny of stakeholders through a meaningful consultation and comment process.
76. CCTA further submits that a "fast-track" approach to drafting and enacting any lawful access legislation and regulations is unwarranted in light of the positive and effective working relationships between law enforcement and carriers/ISPs and given the speed at which equipment and software manufacturers are

*Canadian Cable Television Association*  
*Comments on Lawful Access Consultation Document*  
*December 16, 2002*  
*Page 30 of 30*

excepted to respond to similar legislative initiatives in the U.S. As noted earlier, in the U.S. only voice telephony providers are currently subject to CALEA. Until American ISPs are subject to the requirement to ensure basic intercept capability, there is little likelihood that intercept solutions for Internet providers will become available on a widespread and cost-effective basis throughout North America.

77. CCTA appreciates the opportunity to provide these comments and would be pleased to provide any further assistance the Departments may consider appropriate. Assistance may also be available from experts from within the CCTA membership to serve on any technical advisory committees, should these be established in connection with this legislation.

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Dec 16 3:22 PM  
**To:** la-al@justice.gc.ca  
**Subject:** Lawful Access Consultation Document

s.19(1)

**Importance:** High



Untitled Attachment



Lawful  
Access\_16dec02.doc

s.19(1)

**Pierlot, Paul**

Attached please find the written comments of the Canadian Association of Internet Providers ("CAIP") with respect to the above-noted Lawful Access Consultation Document ("the Consultation Document"), as issued by the Department of Justice, Industry Canada and the Solicitor General Canada on August 25, 2002.

Hard copy to follow by courier.

[REDACTED]  
Executive Administrative Assistant to the  
President & Director of Member Services  
CAIP (Cdn. Assoc. of Internet Providers)  
176 Bronson Avenue - Pollack Place - Ground Floor  
OTTAWA, Ontario [CANADA] K1R 6H4  
Tel.: 613 232 CAIP (2247) Fax: 613 236 9241  
e-mail: [REDACTED] <http://www.caip.ca>

PLEASE NOTE: MY LAST DAY @ CAIP IS FRIDAY, DECEMBER 20th - SO UNTIL THEN ...

- ~ Work like you don't need the money
  - ~ Love like you've never been hurt; and
  - ~ Dance like nobody's watching !
- [REDACTED]

**CAIP**  
Canadian Association  
of Internet Providers



**ACFI**  
Association canadienne  
des fournisseurs Internet

Lawful Access Consultation  
Criminal Law Policy Section  
284 Wellington Street – 5<sup>th</sup> Floor  
Ottawa, Ontario K1A 0H8

e-mail: [la-al@justice.gc.ca](mailto:la-al@justice.gc.ca)

To Whom it May Concern:

**Re: Lawful Access Consultation Document**

Attached please find the written comments of the Canadian Association of Internet Providers ("CAIP") with respect to the above-noted Lawful Access Consultation Document ("the Consultation Document"), as issued by the Department of Justice, Industry Canada and the Solicitor General Canada on August 25, 2002.

The Canadian Association of Internet Providers (CAIP) is the only non-profit association representing all sectors of the Internet provider industry. Our membership is made up of a broad and diverse group of Canadian Internet Service Providers (ISPs), including large, medium and small independent access providers; incumbent and competitive telephone companies; backbone providers; wireless providers and web hosts. CAIP's members currently provide approximately 80% of the Internet connections to Canadian homes, schools and businesses.

The Association's larger members include AOL Canada, AT&T Canada, Bell Canada, IBM, Sprint Canada, Telus and WorldCom Canada. CAIP's Mission is to foster the growth of a healthy and competitive Internet service industry through collective and cooperative action on Canadian and international Internet issues. To this end, we represent our member companies before the federal government and such public authorities as the CRTC, the Copyright Board and the Competition Bureau as well as the federal courts. We actively participate in proceedings, meetings and debates relating to Internet self-regulation, high-speed access, ISP liability, Internet security and law enforcement, e-commerce policy and copyright.

CAIP and its members have a well-deserved reputation for cooperating with the Government of Canada and with law enforcement in our joint efforts to make the Internet a safe place for Canadians. It is with this continuing spirit of cooperation that we file the attached comments and look forward to participating in further consultations regarding these important matters.

Sincerely,

  
President and CEO

s.19(1)

Attachment



## **CAIP Response to Lawful Access Consultation Document: Executive Summary**

### **CAIP's General Position**

CAIP acknowledges lawful access as a tool for use by Canadian law enforcement and national security agencies, subject to the rights, privileges and protections accorded Canadians under the Charter. We support the notion that Canadian law enforcement and national security agencies should, with respect to new communications technologies, have an ability to undertake the lawful interception of communications and search and seizure of information which is equivalent to what they are currently able to undertake with respect to traditional communications technologies such as the public switched telephone network (PSTN) and surface mail. We accept that this tool may need to be updated to ensure it retains its effectiveness in light of new communications technologies.

Based on the consultation process, however, we are not convinced that the lawful access ability does not already exist, at least with respect to the Internet and Canadian ISPs, which represent CAIP's primary constituency.

We remain constrained, however, in our ability to provide constructive and meaningful input in this process because the meaning, scope and potential impact of the proposals remain unclear. Thus, even if there is indeed a need to legislate industry cooperation in the provision of lawful access, we have great difficulty at the present time in offering much more than principled responses to the government's proposals and questions as they relate to the mechanics of possible legislation.

### **COMMENTS**

#### **LEGISLATIVE PROPOSALS**

##### **1. Infrastructure Capability**

###### **Requirement to Ensure Intercept Capability**

The Consultation Document states that service providers would be required to have the technical capability to provide access to "the entirety of a specific telecommunication transmitted over their facilities", subject to a lawful authority to intercept. This "entirety" concept is considerably broad in scope. We require more details regarding its meaning.

###### **A. General Requirements**

The Consultation Document proposes that all service providers would be required to provide, at a minimum, "a basic intercept capability" before providing "new services" or "a significantly upgraded service" to the public. However, these terms and the obligations that would arise from them have not been defined. Thus we have no way to measure their impact from a financial or operational standpoint, and thus no basis on which to make a judgment as to whether the obligations are possible or acceptable.

###### **B. Regulations**

The Consultation Document suggests that the regulations could address the technical and other standards or requirements for service providers, what service providers must do to provide access to their facilities, and issues related to costs. These are the very type of matters which

are of overwhelming concern to service providers in this process and, depending on how they are addressed, will serve the basis for industry players to determine whether and to what extent they can support or must oppose the lawful access proposals. For these reasons, we are concerned that, if relegated to subordinate legislation, they will not be subject to the level of parliamentary review and attention necessary to ensure a full and open assessment of their impact and appropriateness.

We also wish to highlight our concern that the proposals seem to contemplate a "one-size-fits-all" model. This approach will not work given the wide range of service providers in terms of their size, services offered, technical capabilities and operational sophistication.

CAIP recommends that, rather than establishing a regime whereby technical standards and details are specified in regulations, the enabling lawful access legislation establish the legal obligations *and provide for industry-government working groups* to develop the appropriate standards to meet their obligations.

The Government should ensure that service providers are compensated for all the new costs they will have to bear in order to comply with the obligations which will ultimately be established to aid law enforcement once this consultation and legislative process is complete. There should be an explicit recognition that fees are payable to service providers for cost recovery. We don't believe, however, that such compensation could be "tariffed" by way of regulations; instead, the amount of such compensation should be worked out between the service provider and the law enforcement agency on a case-by-case basis.

#### **C. Forbearance**

CAIP supports the principle that service providers should have the opportunity to demonstrate that, based on their special circumstances, they should be forborne from the intercept capability obligations. We recommend that there be flexibility to grant extensions to a forbearance order on a case-by-case basis as well as to grant forbearance to a class or classes of service providers where it can be demonstrated that to do so would be appropriate in the circumstances. The burden of proof, however, must always be on the applicant(s) to demonstrate that the type or extent of the order they seek is clearly in the public interest and that forbearance will eventually give way to compliance.

Before granting any forbearance order, the Government must be satisfied that doing so would not confer an unfair competitive advantage on the recipient(s).

#### **D. Compliance Mechanism**

Sanctions should only be imposed if a service provider was unable or unwilling to meet its obligations after being served by a law enforcement officer with the proper judicial authorization to conduct a lawful intercept. We strongly oppose any system which would require or permit regular or random inspections or analyses to ascertain compliance: such a system would be unduly costly, both for service providers and law enforcement, and would create a whole new level of bureaucracy which would divert resources away from more pressing law enforcement activities. We also oppose any system which would require service providers to register their compliance with law enforcement or a third party, as this would constitute an unnecessary form of industry regulation and again add new costs and a new level of bureaucracy to the system.

#### **E. Cost of Ensuring Intercept Capability**

Absent more details respecting what is required technically and operationally to provide "basic intercept capability", we simply do not have enough information to assess the potential financial impact of these proposals.

The Government should ensure that service providers are compensated for all the new costs they will have to bear in order to comply with the obligations which will ultimately be established to aid law enforcement once this consultation and legislative process is complete. Federal funding must be made available to service providers to retrofit all networks and systems to satisfy the lawful access needs of law enforcement and national security agencies, and to cover all incremental costs to provide the capability for lawful access to new networks and systems providing upgraded, significantly enhanced and new services.

## **2. Amendments to the Criminal Code and other Statutes**

### **A. Production Orders**

#### **i) General Production Orders**

Service providers should be compensated for the costs they incur in order to provide operational assistance in response to a production order.

Such orders should be reasonably executed, taking into account the complexity and the format of the documents and the time it would take a reasonable person to be able to produce them.

CAIP opposes "anticipatory orders" since they would appear to impose an obligation on a custodian to produce documents not yet within its possession and perhaps not likely to come into its possession in the normal course of its business or activities.

All the same procedural safeguards currently applicable to intercept orders should apply with respect to records of content and unopened or unviewed communications. The same procedural safeguards currently applicable to search warrants should apply to data in the possession of the service provider.

#### **ii) Specific Production Orders**

There should be no lowering of the judicial standard for accessing any Internet data which could reveal or be associated with a customer's personal information or directly or indirectly reveal the content of a communication. All the same procedural safeguards currently applicable to intercept orders should be maintained where there is any possibility that the data relates or provides access to the content of a communication or could be used or manipulated to determine or suggest the content of a communication.

CAIP supports the definition of "traffic data" contained in the Council of Europe's Convention on Cybercrime: "any computer data relating to a communications by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."

### **B. Orders to obtain subscriber and/or service provider information**

We are comfortable with the notion of a customer name and address (CNA) order; moreover, since we do not foresee how such an order would result in the disclosure of or access to the content of communications, we are also comfortable with such orders being subject to a lower judicial standard.

No obligations, however, should be imposed on service providers to collect, retain or produce information that they are not already collecting or have in their possession for their own business purposes. Businesses should be free to conduct their businesses as they see fit, within the

parameters of the law, but should not be obliged to take on obligations that are solely of interest to law enforcement and serve no business purpose. Moreover, the standards for accuracy required should be no greater than what is required for commercial operations.

### **C. Assistance orders**

The draft legislation in this area must spell out specifically what would be required of service providers subject to assistance orders; once we have seen such details, we'll be in a better position to assess whether assistance orders are appropriate or not.

### **D. Data-preservation orders**

CAIP supports in principle the notion of a preservation order which, once issued by the proper judicial authority, would require a service provider to ensure that existing specified information in relation to a particular subscriber, and already in the service provider's possession as a result of its normal business practices, is not deleted for a specified, limited period of time.

Service providers must be clearly exempt from criminal or civil liability for actions taken to comply with judicial orders such as data-preservation orders.

It should be clear that data preserved pursuant to a preservation order will only be accessible by the appropriate legal agency or agencies for criminal or national security purposes and will not be accessible by such agencies or any other person or organization for any other purpose or any other legal process, such as a civil subpoena.

Since, in themselves, data preservation orders do not permit law enforcement to access any data, it may not be necessary to apply to them all the same procedural safeguards currently applicable to search warrants. It is still important, however, that there be reasonable constraints on the ability of law enforcement to obtain data-preservation orders to ensure they are not used in a burdensome manner or for frivolous purposes. Accordingly, at a minimum, law enforcement should have to demonstrate to the same judicial authority responsible for issuing search warrants that the records requested to be preserved are proportional and relevant to the investigation, and that compliance with the order would not be unreasonably burdensome on the recipient service provider.

Preservation orders should be valid for no more than 90 days, as per the Cybercrime Convention.

### **E. Virus Dissemination**

Our support for these proposals would be contingent on Canada stipulating that the authorized testing or protection of a computer system is permitted, as per the Cybercrime Convention. It must also be clarified that no ISP would be liable under these provisions for any offence relating to the possession, etc., of a virus absent proof that the ISP had knowledge of the virus and intended to possess it, etc.

### **F. Interception of e-mail**

The "interception" provisions of the *Criminal Code* should apply with respect to records of content and unopened or unviewed communications, including e-mails. The same procedural safeguards currently applicable to search warrants should apply to data, including opened e-mails, in the possession of a person.

### **G. Amendments to the *Competition Act*: Access to Hidden Records/Other Orders**

CAIP has no specific comments in this area, beyond our support for the general principle that sufficient safeguards be included in any provisions relating to evidence gathering, including search and seizure.

#### **3. Other mechanisms to provide subscriber and service provider information**

We oppose in the strongest terms any sort of national database of, e.g., Internet users. We believe such a database would be difficult to establish and nearly impossible to keep up to date, and would place an unreasonable administrative and legal burden on ISPs. More importantly, contrary to the terms and spirit of PIPEDA, it would represent a totally unacceptable invasion of privacy for Canadian Internet users, who should be free to enjoy their use of the Internet without having to be registered with the police.

## **CAIP Response to the Lawful Access Consultation Document December 16, 2002**

### **Background: The Consultation Process**

The Canadian Association of Internet Providers (CAIP) participated in a bilateral meeting with departmental officials on October 16, 2002 and was also represented at the bilateral meeting with representatives of civil liberties groups and privacy advocates which was held on October 21, 2002.

On November 1, 2002, we wrote to the Minister of Justice to express concern that, while we appreciated the officials' efforts to brief us on the Lawful Access Consultation Document ("the Consultation Document"), we found ourselves left with more questions than answers. As a result, we stated, we anticipated we would be unable to provide a meaningful, comprehensive and constructive response to the lawful access proposals until we were able to review the proposed legislation and accompanying regulations. We advised the Minister that, without access to these important documents and the details and definitions we expect they will provide regarding service provider obligations, we would have no way of assessing the potential financial and operational impact of the proposals. We therefore asked that the draft legislation and accompanying regulations be made available for a full and complete public review and that sufficient time be provided for interested parties to assess their impact and submit comments.

### **CAIP's General Position**

CAIP acknowledges lawful access as a tool for use by Canadian law enforcement and national security agencies, subject to the rights, privileges and protections accorded Canadians under the Charter. We support the notion that Canadian law enforcement and national security agencies should, with respect to new communications technologies, have an ability to undertake the lawful interception of communications and search and seizure of information which is equivalent to what they are currently able to undertake with respect to traditional communications technologies such as the public switched telephone network (PSTN) and surface mail. We accept that this tool may need to be updated to ensure it retains its effectiveness in light of new communications technologies.

Based on the consultation process, however, we are not convinced that the lawful access ability does not already exist, at least with respect to the Internet and Canadian ISPs, which represent CAIP's primary constituency.

While the Consultation Document indicates that law enforcement may experience problems in obtaining lawful access to the Internet - the same suggestion was echoed by some officials during the stakeholder meetings - we have yet to be offered concrete examples of where such difficulties have arisen, or statistics or other data which would support such assertions. To the contrary, we were advised during the CAIP stakeholder meeting that Canadian ISPs provided few if any problems for law enforcement officers seeking lawful access and were in fact generally cooperative and helpful when called upon to assist in investigations.

CAIP and its members - and Canadian ISPs generally - wish to maintain the positive working relationship that the industry has built up with law enforcement over the years, and are quite prepared to continue to help out in investigations where possible and appropriate and where proper judicial procedures are followed. It is on this basis that we have participated in the consultation process, that we offer the following comments in response to the Consultation Document and that we intend to participate in the public process(es) which will arise with respect to the draft legislation and accompanying regulations once they are tabled.

Nevertheless, as noted above, in participating at least in these first stages of the process, we are constrained in our ability to provide constructive and meaningful input because we find that the meaning, scope and potential impact of the proposals remain unclear. In many ways, what are proposed in the Consultation Document are principles, with few details regarding implementation and impact. We've been advised that the details will be set out in the legislation and the accompanying regulations. Without these details, however, we are unable to do much more than offer principled positions in response. Thus, even if there is indeed a need to legislate industry cooperation in the provision of lawful access, we have great difficulty in offering much more than principled responses to the government's proposals and questions as they relate to the mechanics of possible legislation.

We look forward to the opportunity to examine and consider the legislation and regulations which will ultimately flow from the Consultation Document, and we anticipate being in a position to respond in a more detailed manner at that time.

## **COMMENTS**

### **LEGISLATIVE PROPOSALS**

#### **1. Infrastructure Capability**

##### **Requirement to Ensure Intercept Capability**

The Consultation Document notes at the outset that there is currently no legislative mechanism in Canada that can be used to compel service providers to develop or deploy systems providing interception capability. The document suggests that legislation is therefore necessary. As noted at the outset of these comments, we have yet to see overwhelming (if any) evidence that a problem exists as regards Internet service providers; accordingly, we find it difficult to accept that new laws are in fact needed in this area. Moreover, we cannot offer support for legislation when, as in the present case, we lack sufficient detail to measure or assess its potential financial and operational impact on our members.

The Consultation Document states that the "central tenet" of the proposal is that service providers would be required to have the technical capability to provide access to "the entirety of a specific telecommunication transmitted over their facilities", subject to a lawful authority to intercept. The Document also states that the entirety of telecommunication includes the content and the telecommunications-associated specific data associated with the telecommunication.

This "entirety" concept is considerably broad in scope. We require more details regarding its meaning. For example, what constitutes a "specific telecommunication": is it a single e-mail message? A request for a web page? Could it encompass a series of messages from or to a specific user? Does it include responses, if any? What would a service provider's obligations be if a "specific telecommunication" took on different forms, was copied in different formats or applications or was routed through a number of different parts of the network? Would this mean the service provider would have to make every component of its network and facilities accessible for law enforcement to intercept the telecommunication?

##### **A. General Requirements**

The Consultation Document proposes that all service providers would be required to provide, at a minimum, "a basic intercept capability" before providing "new services" or "a significantly upgraded service" to the public.

Despite frequent requests from various stakeholders during the consultation process, however, officials were unable to provide a comprehensive definition of what constitutes a "basic intercept



capability". Similarly, stakeholders were often left with more questions than answers with respect to what constitutes "new services" versus old or existing ones, or at what point an existing service will be considered to have been "significantly upgraded". These latter two definitions take on even greater significance in light of the cost implications they will present to service providers (discussed further below).

In presentations delivered to the different stakeholder groups, officials indicated that basic intercept capability would *include* 'real-time' monitoring. Beyond that, we were advised only that the legislation/regulations would set out obligations respecting:

- methods to correlate the intercepted data and content;
- the number of simultaneous interceptions;
- interfaces, delivery methods and formats;
- service provider initiated encryption;
- quality of service;
- location information;
- physical personnel and administrative security measures; and
- access to subscriber/customer information.

We received no details, however, regarding these obligations; accordingly, as we advised the Minister in our November 1 letter, we have no way to measure their impact from a financial or operational standpoint, and thus no basis on which to make a judgment as to whether they are possible or acceptable.

## **B. Regulations**

The first line of this paragraph states: "It is crucial that service providers know what is required of them." We couldn't agree more. The fact that we still do not know what will be required of service providers means that the Government must provide much more information and more time to assess it.

It is not an uncommon approach to establish general obligations within a governing piece of legislation and then to establish operational and technical details in accompanying regulations, as is proposed here. We are reluctant, however, to offer our support for such an approach in the present context since it appears to us that the crucial elements of the obligations would be contained in the regulations.

The Consultation Document suggests that the matters addressed in the regulations could include the technical and other standards or requirements for service providers, what service providers must do to provide access to their facilities, and issues related to costs. These are the very type of matters which are of overwhelming concern to service providers in this process and, depending on how they are addressed, will serve the basis for industry players to determine whether and to what extent they can support or must oppose the lawful access proposals. For these reasons, we are concerned that, if relegated to subordinate legislation, they will not be subject to the level of parliamentary review and attention necessary to ensure a full and open assessment of their impact and appropriateness.

We also wish to highlight our concern that the proposals seem to contemplate a "one-size-fits-all" model. The ISP industry in Canada is made up of a broad cross-section of companies: a small handful are large, sophisticated and well staffed; however, by far, most are small or very small, and many are struggling.

In its March 2002 report for Industry Canada ("Industry Framework of Internet Service Providers"), POLLARA Inc. concluded that there are 940 ISPs in Canada, of which about 400 serve more than 1,000 customers each (see [www.caip.ca/issues/ISPReport.pdf](http://www.caip.ca/issues/ISPReport.pdf)). The average



number of employees at an ISP is 6, while 44% of all ISPs have between 1 and 5 employees. The vast majority of ISPs (60.6%) have revenues under \$1 million. Almost 40% have margins of 6% or less. Nearly 1 in 5 ISPs is operating at a loss.

Any lawful access obligations must take into account these divergent circumstances and available resources, and not impose technical or operational obligations which would be impractical to meet or overly burdensome. For example, it is simply not possible for a small ISP struggling to survive with only a handful of employees to insist that those employees meet potentially strict legal obligations relating to their level of competence, reliability and deployment.

The Consultation Document suggests that details and cost matters will be addressed in regulations. As we have pointed out, however, a one-size-fits all approach will not work given the wide range of service providers in terms of their size, services offered, technical capabilities and operational sophistication. Moreover, while regulations are generally more flexible than legislation in that they are typically easier to amend or alter to respond to changing circumstances, they still would ultimately represent a government-imposed approach which may not work in all situations or for all service providers and which may need altering to respond to technological or industry changes in a manner and at a speed which could not be accomplished adequately through the regulation-making process.

Moreover, it is fair to say that industry is in a better position than government or law enforcement to assess cost implications and, accordingly, to devise the most cost-efficient solutions in this area.

For these reasons, CAIP recommends that, rather than establishing a regime whereby technical standards and details are specified in regulations, the enabling lawful access legislation establish the legal obligations and provide for *industry-government working groups to develop the appropriate standards to meet their obligations*. This would be similar to the system which exists in the US under CALEA, and which we understand has led to the successful development of lawful access standards in such areas as paging, cable telephony, soft switches and PCS phones. In the US, each of the industry-developed standards is deemed to be the acceptable approach unless law enforcement can clearly demonstrate that it does not work.

The CALEA regime is as follows:

**SEC. 107. TECHNICAL REQUIREMENTS AND STANDARDS; EXTENSION OF COMPLIANCE DATE.**

**(a) SAFE HARBOR-**

(1) CONSULTATION- To ensure the efficient and industry-wide implementation of the assistance capability requirements under section 103, the Attorney General, in coordination with other Federal, State, and local law enforcement agencies, shall consult with appropriate associations and standard-setting organizations of the telecommunications industry, with representatives of users of telecommunications equipment, facilities, and services, and with State utility commissions.

(2) COMPLIANCE UNDER ACCEPTED STANDARDS- A telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 103, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 106, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b), to meet the requirements of section 103.

(3) **ABSENCE OF STANDARDS**- The absence of technical requirements or standards for implementing the assistance capability requirements of section 103 shall not--

- (A) preclude a telecommunications carrier, manufacturer, or telecommunications support services provider from deploying a technology or service; or
- (B) relieve a carrier, manufacturer, or telecommunications support services provider of the obligations imposed by section 103 or 106, as applicable.

(b) **COMMISSION AUTHORITY**- If industry associations or standard-setting organizations fail to issue technical requirements or standards or if a Government agency or any other person believes that such requirements or standards are deficient, the agency or person may petition the Commission to establish, by rule, technical requirements or standards that--

- (1) meet the assistance capability requirements of section 103 by cost-effective methods;
- (2) protect the privacy and security of communications not authorized to be intercepted;
- (3) minimize the cost of such compliance on residential ratepayers;
- (4) serve the policy of the United States to encourage the provision of new technologies and services to the public; and
- (5) provide a reasonable time and conditions for compliance with and the transition to any new standard, including defining the obligations of telecommunications carriers under section 103 during any transition period.

Canada, and the telecom service provider industry in particular, are very well positioned to take on this standard-setting function given the industry's lengthy experience with similar arrangements in addressing telecom regulatory matters.

In our opinion, this approach, which has succeeded to date in the US, would benefit law enforcement, industry and consumers since it would mean that the task of developing the most efficient and cost-effective technical solutions would be assigned to those most knowledgeable and qualified in this area - the experts within industry - while the responsibility to ensure effectiveness would rest with those putting the solutions into practice - law enforcement. CAIP would be prepared to offer its expertise in the government/industry groups.

#### ***Issues to be considered***

1. *How could regulations prescribe technical and other standards or requirements for:*
  - a. *apparatus to be installed, attached or otherwise related to its facility, and the capacity requirements for the maximum number of simultaneous interceptions pertaining to such apparatus?*
  - b. *terms and conditions pertaining to the security of interceptions and of the delivery of the product of interceptions?*
  - c. *the competence, reliability and deployment of employees?*

**Response:** See above recommendation for industry-government working groups to develop standards.

2. *Should regulations provide for fees to be paid to a service provider for operational assistance?*

**Response:** The Government should ensure that service providers are compensated for all the new costs they will have to bear in order to comply with the obligations which will ultimately be established to aid law enforcement once this consultation and legislative process is complete. Law enforcement is the responsibility of the Government through its applicable agencies; therefore the costs of law enforcement should be borne by the Government and not any particular industry or companies.

Accordingly, service providers should recover their costs for providing operational assistance. As noted above, most Canadian ISPs function with minimal staff, and time invested by these employees in functions other than maintaining their network and serving their customers represents a cost to the ISP's business which most ISPs can ill-afford given their already thin margins. New and otherwise unrecoverable costs could also be incurred for such activities as storing data, implementing new management processes, or for the setup and running of related equipment. A system for cost recovery in these circumstances is therefore both appropriate and necessary.

As we understand the current situation with respect to PSTN voice intercepts, some but not all service providers have successfully arranged to be compensated for operational assistance from some but not all law enforcement agencies. In other words, there is no a uniform practice or approach within the industry or law enforcement. In our opinion, there should be an explicit recognition that fees are payable to service providers for cost recovery. We don't believe, however, that such compensation could be "tariffed" by way of regulations, since circumstances could often differ based, for example, on the size and sophistication of the ISP and the extent and scope of the information or access that law enforcement was seeking. For this reason, we believe that once the principle of service provider cost recovery is firmly established, the amount of such compensation should be worked out between the service provider and the law enforcement agency on a case-by-case basis. It may even be possible for general standards to be adopted in this area: perhaps CAIP could help in this regard.

**C. Forbearance**

CAIP supports the principle that service providers should have the opportunity to demonstrate that, based on their special circumstances, they should be forborne from the intercept capability obligations. It is difficult for us to provide more detailed comments on this aspect of the Government's proposals, however, since we have little information as to the type of circumstances under which a service provider might seek forbearance or the range of obligations from which it may wish to be forborne.

We note that the proposal contemplates that a forbearance order would only be for "a limited time". While, depending on the associated obligations, a limited time forbearance order might be sufficient for a particular service provider, there might also be circumstances under which extensions to such an order would be appropriate. For this reason, we recommend that there be flexibility to grant extensions to a forbearance order on a case-by-case basis.

We also note that the proposal appears to contemplate that forbearance orders would only be granted to individual service providers upon application. We envisage, however, that there could be cases in which it might be appropriate to grant a forbearance order to an identified class of service providers. For example, we understand that certain classes of service providers are exempt from the data interception obligations applicable in the United Kingdom, including those which do not intend to supply services to more than 10,000 people in the UK, and financial institutions such as banking, insurance and investment houses. It may be similarly appropriate to exempt these or other classes of service providers in Canada, in recognition of their particular

economic or operational challenges. Accordingly, we recommend that there be flexibility to grant forbearance to a class or classes of service providers where it can be demonstrated that to do so would be appropriate in the circumstances.

In recommending flexibility with respect to the length and subjects of forbearance orders, we are *not* suggesting that unlimited or widely-applicable orders become the norm: the burden of proof must always be on the applicant(s) to demonstrate that the type or extent of the order they seek is clearly in the public interest and that eventually forbearance will give way to compliance.

In addition, before granting any forbearance order, the Government must be satisfied that doing so would not confer an unfair competitive advantage on the recipient(s).

#### **D. Compliance Mechanism**

The Consultation Document correctly points out that any compliance mechanism adopted would need to minimize the costs for both industry and government.

##### ***Issues to be considered***

1. *What kind of compliance mechanism should be established?*
2. *Who should conduct the compliance activities and prescribe the circumstances under which they may be conducted?*
3. *What type of penalty should be provided for in cases where service providers do not comply with the law?*

Response: It should be assumed that service providers will comply with the law and that sanctions would only be imposed if a service provider was unable or unwilling to meet its obligations after being served by a law enforcement officer with the proper judicial authorization to conduct a lawful intercept. We strongly oppose any system which would require or permit regular or random inspections or analyses to ascertain compliance: such a system would be unduly costly, both for service providers and law enforcement, and would create a whole new level of bureaucracy which would divert resources away from more pressing law enforcement activities. We also oppose any system which would require service providers to register their compliance with law enforcement or a third party, as this would constitute an unnecessary form of industry regulation and again add new costs and a new level of bureaucracy to the system.

We do not have specific recommendations as to the nature of the penalty to be imposed for non-compliance, as we are not experts in such matters. We would suggest that the penalty should be such as to represent a sufficient deterrent to not complying with the law without being so onerous as to force a struggling service provider out of business. Service providers should have the opportunity to prove that they were in compliance.

#### **E. Cost of Ensuring Intercept Capability**

The Consultation Document proposes that service providers would be responsible for the costs associated with providing the lawful access capability for "new technologies" or when a "significant upgrade" is made to their systems or networks. Service providers would not be required to pay for necessary changes to their existing systems or networks. The Document is not clear, however, as to whether the obligation to provide "basic intercept capability" nevertheless still applies with respect to existing systems or networks and, if it does, as to who would pay for the "necessary changes".

As noted earlier, neither the Consultation Document nor the various stakeholder meetings have provided sufficient clarity with respect to what constitutes "new" technologies or a "significant upgrade". Absent more details respecting the meaning of these phrases as well as what is

required technically and operationally to provide "basic intercept capability", we simply do not have enough information to assess the potential financial impact of these proposals. We are aware, however, of a recent IDC Canada report which suggests that the associated costs could be substantial and could, as a result, drive smaller ISPs out of business. We also understand that knowledgeable observers in the US have suggested that implementation of their lawful access legislation (in CALEA) could cost the industry upwards of \$1 billion. Obviously, the Canadian industry could not afford anywhere near that amount, and any cost that would threaten to drive smaller operators out of business would simply be untenable.

As stated earlier, we believe the Government should ensure that service providers are compensated for all the new costs they will have to bear in order to comply with the obligations which will ultimately be established to aid law enforcement once this consultation and legislative process is complete. Law enforcement is the responsibility of the Government through its applicable agencies and so the costs of law enforcement should be borne by the Government and not any particular industry or companies. For this reason, and in light of the serious impact the new associated costs could have on the service provider industry, we submit that sufficient federal funding must be made available to service providers:

- to retrofit all networks and systems to satisfy the lawful access needs of law enforcement and national security agencies; and
- to cover all incremental costs to provide the capability for lawful access to new networks and systems providing upgraded, significantly enhanced and new services.

## **2. Amendments to the *Criminal Code* and other Statutes**

CAIP has no particular expertise with respect to the *Criminal Code* or criminal or lawful investigation procedures as provided for under the Code or under other federal legislation. Accordingly, we're not in a position to provide in-depth analysis of the proposals in this section of the Consultation Document or detailed comments in response. Nevertheless, we've attempted to offer our input where possible.

As with all of our comments in this paper, we reserve the right to alter any or all of our positions if we deem it appropriate in light of the submissions of other interested parties in this process.

### **A. Production Orders**

#### **i) General Production Orders**

The Consultation Document proposes the creation of a general production order which would require the custodian of identified document(s) to deliver or make available the document(s) to law enforcement officials within a certain period of time. The Consultation Document identifies the "problem" which such orders would be intended to solve as arising when a third-party takes "some time" to find and produce requested documents.

While we agree that a production order could be less intrusive than a search warrant as there would be no entry into and search of the custodian's premises, we are concerned that the primary motivation seems to be to force custodian to produce documents in an expedited manner. No consideration appears to be given to the possible difficulties a custodian might have in accessing the documents to produce or to any limitations that should be placed on the extent, breadth or volume of the documents that could be sought.

As noted earlier, service providers should be compensated for the costs they incur in order to provide operational assistance, in this case in response to a production order.

### ***Issues to be considered***

1. *Should the Criminal Code be amended to allow law enforcement officials to obtain production orders in specific cases?*

Response: We have no opinion on the need or appropriateness of general production orders. However, should they be introduced, they should be reasonably executed, taking into account the complexity and the format of the documents and the time it would take a reasonable person to be able to produce them.

2. *Should the Criminal Code allow for anticipatory orders (e.g., permit law enforcement agencies to monitor transactions for a specified period of time)?*

Response: An "anticipatory order" would appear to be substantially different from a production order since the latter requires the production of documents already in a custodian's possession while the former would appear to impose an obligation on a custodian to produce documents not yet within its possession and perhaps not likely to come into its possession in the normal course of its business or activities. CAIP opposes such a vague and potentially far-reaching proposal.

3. *What kind of procedural safeguards should be included?*

Response: All the same procedural safeguards currently applicable to intercept orders should apply with respect to records of content and unopened or unviewed communications. The same procedural safeguards currently applicable to search warrants should apply to data in the possession of the service provider.

### ***ii) Specific Production Orders***

We are generally uncomfortable with any lowering of the judicial standards associated with seeking or obtaining information in the course of a police investigation. The Consultation Document notes that, except in certain "very limited cases, the current safeguard prevents important information from being gathered at an early investigation stage, even if there is a low expectation of privacy in relation to the information being sought." We assume that the current safeguard applies in these circumstances for a legitimate reason and we strongly suggest caution should be exercised when considering changes. Without supporting evidence, we do not accept that a lower expectation of privacy automatically exists with respect to the additional forms of information under consideration in this section. We also do not readily accept that there is a lower expectation of privacy in any Internet-related data that could reveal or be associated with a customer's personal information.

### ***Issues to be considered***

1. *Should there be a specific power, parallel to that provided for in the Criminal Code dial number recorders, to allow law enforcement and national security agencies to obtain traffic data?*
2. *How should "traffic data" be defined? Should the definition of traffic data be combined with telephone-related information and addressed in the same Criminal Code provision?*
3. *Should other specific production orders be created under a lower standard?*
4. *What kind of procedural safeguards should be included?*

Response: There should be no lowering of the standard for any Internet data which could reveal or be associated with a customer's personal information or directly or indirectly reveal the content of a communication. All the same procedural safeguards currently applicable to intercept orders should be maintained where there is any possibility that the data relates or provides access to the



content of a communication or could be used or manipulated to determine or suggest the content of a communication.

The Council of Europe's Convention on Cybercrime defines "traffic data" with respect to the Internet to mean "any computer data relating to a communications by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service." The Explanatory Report to the Convention points out that not all of these categories will always be technically available, capable of being produced by a service provider, or necessary for a particular criminal investigation. The Report also explains that the "origin" refers to a telephone number, the Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services; the "destination" refers to a comparable indication of a communications facility to which communications are transmitted; and the term "type of underlying service" refers to the type of service that is being used within the network, e.g. file transfer, electronic mail, or instant messaging.

CAIP considers that Canada should adopt this same definition, as explained in the Convention's Explanatory Notes.

## **B. Orders to obtain subscriber and/or service provider information**

### ***Issues to be considered***

1. *Should there be a specific production order in relation to customer name and address and service provider information?*
2. *Under what conditions should such information be made available and to whom?*
3. *What is the standard that should be required?*
4. *Should this obligation be imposed even if the service provider is not currently collecting this information for its own purposes?*

Response: There should be no lowering of the standard for any Internet data which could reveal or be associated with a customer's personal information or directly or indirectly reveal the content of a communication. All the same procedural safeguards currently applicable to intercept orders should be maintained where there is any possibility that the data relates or provides access to the content of a communication or could be used or manipulated to determine or suggest the content of a communication.

We are comfortable with the notion of a CNA order; moreover, since we do not foresee how such an order would result in the disclosure of or access to the content of communications, we are also comfortable with such orders being subject to a lower standard.

No obligations, however, should be imposed on service providers to collect, retain or produce information that they are not already collecting or have in their possession for their own business purposes. A clear distinction must be made between businesses which comply with the law and agencies or officers which enforce the law. Service providers are businesses and should not be allocated the task of law enforcement. Businesses should be free to conduct their businesses as they see fit, within the parameters of the law, but should not be obliged to take on obligations that are solely of interest to law enforcement and serve no business purpose. Moreover, the standards for accuracy required should be no greater than what is required for commercial operations.

## C. Assistance orders

### *Issues to be considered*

1. *Should legislation that already allows for the issuance of search warrants or the granting of interception authorizations be amended to include the possibility for a judge or justice to issue an assistance order to give effect to the warrant or authorization?*
2. *Should assistance orders more clearly spell out the scope and limits of what a person may be required to do to give effect to the warrant or authorization?*

Response: The Consultation Document notes that some stakeholders have suggested that any Act allowing for the issuance of assistance orders should spell out what could specifically be required under such orders and that, in the context of lawful access, such clarification of the law could allow service providers to understand more clearly the extent of their obligations. CAIP agrees wholeheartedly that the draft legislation in this area must spell out specifically what would be required of service providers subject to assistance orders; once we have seen such details, we'll be in a better position to assess whether assistance orders are appropriate or not.

## D. Data-preservation orders

Subject to the following comments, CAIP supports in principle the notion of a preservation order which, once issued by the proper judicial authority, would require a service provider to ensure that existing specified information in relation to a particular subscriber, and already in the service provider's possession as a result of its normal business practices, is not deleted for a specified, limited period of time.

Service providers must be clearly exempt from criminal or civil liability for actions taken to comply with judicial orders such as data-preservation orders. To this end, we note that Canada's *Anti-Terrorism Act* specifically provides that "no criminal or civil proceedings lie against a person" for action required to comply with the disclosure provisions of the Act when "made in good faith".

It should be recognized that service providers could possibly incur substantial costs in order to comply with a preservation order. For this reason, law enforcement should always first consider the availability and usefulness of investigative means other than preservation, and of using publicly available data. If a preservation order is the only available investigative means in the circumstances, service providers should, as recommended earlier, be compensated for their associated costs. We would suggest that these costs could, and should, be limited by, amongst other things, ensuring that:

- requests for preservation of data are limited in scope, to the extent possible;
- requests are articulated in precise and understandable language;
- where possible, electronic requests (e.g. by e-mail), if authorized, incorporate appropriate authentication technique; and
- the format for the orders is standardized (in order to minimize the need for analysis by providers).

It should also be clear that a service provider would be justified, under specified circumstances, to seek clarification or modification of a preservation order or even to refuse to comply with such an order. To this end, it should be clear as to what authority can resolve disputes relating to the validity or scope of a preservation order.

Law enforcement should be under a duty to revoke a preservation order in a timely manner when it becomes clear that they no longer believe that a related disclosure will follow.



It should be clear that data preserved pursuant to a preservation order will only be accessible by the appropriate legal agency or agencies for criminal or national security purposes and will not be accessible by such agencies or any other person or organization for any other purpose or any other legal process, such as a civil subpoena.

### ***Issues to be considered***

1. *Should a data-preservation order apply only to stored computer data or should it also apply to paper records?*
2. *Under what legal standard should a data-preservation order be granted?*
3. *Should standards vary depending on the nature of the data?*
4. *Who should be authorized to issue a preservation order?*
5. *What is a reasonable period for a custodian of data to be compelled to preserve data: 90, 120, 180 days?*
6. *Should there be a specific penalty for non-compliance with a preservation order, or is contempt of court sufficient?*
7. *For how long should a law enforcement official be able to impose a preservation order on service providers in exigent circumstances?*

**Response:** Since, in themselves, data preservation orders do not permit law enforcement to access any data, it may not be necessary to apply to them all the same procedural safeguards currently applicable to search warrants. It is still important, however, that there be reasonable constraints on the ability of law enforcement to obtain data-preservation orders to ensure they are not used in a burdensome manner or for frivolous purposes. Accordingly, at a minimum, law enforcement should have to demonstrate to the same judicial authority responsible for issuing search warrants that the records requested to be preserved are proportional and relevant to the investigation, and that compliance with the order would not be unreasonably burdensome on the recipient service provider.

Article 16 (2) of the Council of Europe's Convention on Cybercrime stipulates that preservation orders may only be issued for "up to a maximum of 90 days". Accordingly, Canada should not adopt any lengthier period, and may wish to consider a shorter period. Law enforcement should be required to meet the same standard as met for the initial order before an expiring order may be renewed.

Contempt of court would seem to be a sufficient sanction for non-compliance with a preservation order. The standard form for the preservation order should indicate that this is the penalty for non-compliance.

The Consultation Document suggests 4 days as the period for data preservation in exigent circumstances. This seems reasonable. Given that exigent circumstances are those which suggest *immediate* action is necessary, e.g. to protect life, we would certainly not envisage any lengthier a time period.

### **E. Virus Dissemination**

The Consultation Document proposes that the *Criminal Code* be amended to

- clarify that the creation, sale and possession of a computer virus program for the purpose of committing a computer offence or mischief is an offence;
- create new offences in relation to illegal devices (such as viruses), including importation, procurement for use and otherwise making available a device as defined the Cybercrime Convention.

We note that subsection (2) of Article 6 of the Cybercrime Convention, which covers this particular subject under the title "Misuse of Devices", provides that the article shall not be interpreted as imposing liability where the otherwise prohibited activity would not be for the purpose of committing an offence, such as for the authorized testing or protection of a computer system. This is an important limitation and our support for the proposals immediately above would be contingent on the same limitation being adopted in Canada and explicitly enunciated in the legislation.

It must be clarified that no ISP would be liable under these provisions for any offence relating to the possession, etc., of a virus absent proof that the ISP had knowledge of the virus and intended to possess it, etc.

#### **F. Interception of e-mail**

The Consultation Document summarizes current problems associated with determining whether and at what stage in the communication process the judicially-authorized access to an e-mail message should fall under either the "search and seizure" or "interception" provisions of the *Criminal Code*.

##### ***Issues to be considered***

1. *Should there be a specific provision in the Criminal Code in relation to how an e-mail should be acquired?*
3. *If such a provision should be included, what kind of procedural safeguards should be imposed?*
4. *Should the type of order to be obtained in order to acquire an e-mail vary depending on the stage of the communication or delivery process?*

**Response:** The "interception" provisions should apply with respect to records of content and unopened or unviewed communications, including e-mails. The same procedural safeguards currently applicable to search warrants should apply to data, including opened e-mails, in the possession of a person.

#### **F. Amendments to the Competition Act: Access to Hidden Records/Other Orders**

The Consultation Document proposes that the *Competition Act* be amended so as to provide for the capability of requesting persons found on a search premises to provide any records hidden on their person, including hidden electronic and digital devices or media mentioned in the search warrant, to officers on the premises; and provide for an obstruction provision specific to those failing to comply. The Document also proposes that Competition officers be granted the ability to obtain general warrants and assistance orders to enhance the efficiency of evidence gathering tools.

CAIP has no specific comments in this area, beyond our support for the general principle that sufficient safeguards be included in any provisions relating to evidence gathering, including search and seizure.

#### **3. Other mechanisms to provide subscriber and service provider information**

This final section of the Consultation Document considers means by which law enforcement and national security agencies could obtain access to information on the subjects of their investigations, including local service provider identification (LSPID) information and customer name and address (CNA) information. Reference is made to a recommendation from the Canadian Association of Chiefs of Police that a national database be established.

### **Issues to be considered**

1. *What type of mechanism, if any, should be put in place to provide law enforcement and national security agencies with up-to-date and accurate CNA and LSPID information while respecting the privacy of Canadians?*
2. *Should an obligation to collect such CNA information be imposed even if the service provider does not collect this information for its own purposes? In other words, should a provider be compelled by law to collect CNA information?*
3. *Some mechanisms with respect to CNA information are already in place with respect to telephones. Should such mechanisms be created or adapted to provide similar subscriber information for Internet service providers?*
4. *Who should pay the costs of collecting, retaining and accessing this information?*
5. *If a database were to be established, who should operate this database?*

Response: CAIP is very concerned about the privacy and business confidentiality implications of this discussion in the Consultation Document. We oppose in the strongest terms any sort of national database of, e.g., Internet users. We believe such a database would be difficult to establish and nearly impossible to keep up to date, and would place an unreasonable administrative and legal burden on ISPs. More importantly, contrary to the terms and spirit of PIPEDA, it would represent a totally unacceptable invasion of privacy for Canadian Internet users, who should be free to enjoy their use of the Internet without having to be registered with the police.

Telecom service providers should not be obliged to undertake actions or collect information solely for law enforcement purposes, i.e. which they would not otherwise do for their own business purposes. Not only would this impose costs upon the service provider – and by extension upon their customers – it would represent a forced delegation of the law enforcement function to industry. It is the responsibility of industry to comply with Canada's laws; it is the responsibility of law enforcement agencies, not industry, to enforce them.

All of which is respectfully submitted this 16<sup>th</sup> day of December 2002.

JUSTICE DEPT\Lawful Access\_16dec02.doc

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Dec 16 3:33 PM s.19(1)  
**To:** la-al@justice.gc.ca  
**Subject:** Submission document  
**Importance:** High

**CONFIDENTIAL**

December 16, 2002

Lawful Access Consultation

Criminal Law Policy Section

5<sup>th</sup> Floor, 284 Wellington Street

Ottawa, Ontario

K1A 0H8

Dear Sir/Madam:

Attached is a copy of Yahoo Canada Co.'s submission in response to the August 25, 2002 Lawful Access consultation document. A copy has also been forwarded by regular mail.

We request that the submission be held in the strictest confidence and not be made public given the business sensitivity of the subject matter.

Please feel free to contact me if there are any issues regarding our request for confidentiality.

Yours truly,

[REDACTED]

Encl.

Yahoo Canada <http://www.yahoo.ca/>

Yahoo Canada en français <http://cf.yahoo.ca/>

2002-12-18

000584

**IMPORTANT NOTICE:** This message is intended only for the use of the individual or entity to which it is addressed, and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient, or the employee or agent responsible for delivering the message to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify Yahoo Canada immediately by email at [REDACTED]

[REDACTED] Thank you.

s.19(1)

***Confidential***  
***Not for publication***

To: Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington Street  
Ottawa  
Ontario  
Canada  
K1A 0H8

16 December 2002

**Response to Lawful Access – Consultation Document**

To Whom It May Concern:

Yahoo! Canada is pleased to have the opportunity to respond to the above consultation document. Yahoo! Canada is a division of Yahoo! Inc., a leading provider of comprehensive online products and services to consumers and businesses worldwide. Yahoo! is the No. 1 Internet brand globally and the most trafficked Internet destination worldwide.

**We would ask that the following comments be treated in strictest confidence, given the business sensitivity of the subject matter.**

Our concerns can be summarized as follows:

General concerns:

- Lack of sufficient justification and evidence to suggest that current lawful access to data held by service providers is inadequate;
- Privacy concerns;
- No discussion of scope of jurisdiction.

Specific concerns:

- Lack of clarity of definitions in the consultation document;
- Cost allocation;
- Proposals concerning other mechanisms to provide data.

**Confidential**  
**Not for publication**

**Lack of sufficient justification and evidence to suggest that current lawful access provisions are inadequate**

While we sympathize with the task faced by law enforcement agencies in the fight against crime and the need for timely access to data, we are unconvinced by the superficial justification made in the consultation paper for increased access powers. Concrete examples of where current and past criminal investigations have failed as a result of a lack of access to data would help clarify why the current system is no longer deemed adequate and would inform necessary remedial action. In addition, there is no evidence in the document that these proposed new powers will improve safety or investigations in a meaningful way and to a measurable degree. Without this, we believe it would be difficult to justify the erosion of Canadian citizens' privacy the new proposals entail.

The fact that Canada is a signatory of the Council of Europe Cybercrime Convention should not be used as a justification for compliance with that instrument. Until the Convention is ratified by Parliament, and it is by no means certain it will do so, it should not be used as a pretext for increasing powers of access. Indeed, despite the large number of signatory states in Budapest in November 2001, only a handful have thus far ratified the Convention in their national parliaments. It is possible that states such as the USA will never do so.

**Privacy concerns**

Current privacy legislation relies on a fine balance between protecting citizens' fundamental right to privacy, the needs of business to process certain data to provide a service and the need for law enforcement to have access to data to be able to adequately conduct criminal investigations. The proposals risk tipping this balance, perhaps irreversibly, in the direction of intrusion by law enforcement. As has been seen in other countries, once privacy laws are eroded they are rarely re-instated.

**No discussion of scope of jurisdiction**

Many service providers in Canada have their own (or make use of others') servers situated outside of Canada. How lawful access laws should apply to user and communications data held on servers located in a foreign jurisdiction should, therefore, be a key question of this consultation.

The UK government has attempted to address this issue in its draft Code of Practice (paragraph 12) on retaining data under the Anti-Terrorism Crime and Security Act 2001. Of particular significance is the final two sentences, which we italicize for clarity below.

"The code of practice applies to all communications providers who provide a public telecommunications service in the United Kingdom as defined in section 2 of the Regulation of Investigatory Powers Act 2000, and who retain communications data in line with the provisions of the 2001 Act. The Secretary of State considers it necessary for the national security purposes outlined in The 2001 Act, for communications data held by communications providers, which relates to subscribers resident in the UK or subscribing

**Confidential**  
**Not for publication**

to or using a UK-based service, to be retained in accordance with the provisions of the code, whether the data are generated or processed in the UK or abroad. *However, if data relating to a service provided in the UK are stored in a foreign jurisdiction it may be subject to conflicting legal requirements prohibiting the retention of data in accordance with this code. In such cases, it is accepted that it may not be possible to adhere to the terms of this code in respect of that communications data.*"

While the UK Code of Practice is only at internal draft stage, it appears that the UK government understands, and accepts, that foreign-hosted data should not be subject to domestic data storage requirements, but rather to the laws of the country in which the data is stored. By implication, the data should therefore continue to be accessed by existing bilateral and multilateral cooperative law enforcement channels. We would urge a similar provision be included in any future Canadian lawful access instrument. To do otherwise, would be to expose service providers to risk of unlawful access in the country in which the data is stored.

**Lack of clarity of definitions**

There is a lack of clarity in some of the definitions contained in the consultation paper. We are unable to determine whether our business would be covered by all, some, or none of the provisions. In particular:

*"service provider" means a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada (page 4).* This definition is so broad as to be practically meaningless. What is the definition of "the public"?

*"transmission facility" means a wire, cable, radio, optical or other electromagnetic system, or any other (similar) technical system, used for the transmission of information between network termination points (page 7).* This appears to apply to "traditional" ISPs offering access services only? Are service providers not offering access, but offering web-based email services supposed to be captured by this definition?

*"telecommunications facility" (i.e. the legislation would apply to all service providers operating a telecommunications facility in Canada)(page 8).* Clearly, not all service providers operate a telecommunications facility. Yahoo! and many others provide online services to the public and to businesses without providing any Internet access facility. In our reading, the proposed legislation would only apply to Internet service providers in the narrowest and traditional sense of the term; that is, companies providing direct access to the Internet via a telecommunications system. If this is the case, then it should be made explicit.

*"telecommunications associated data" means any data, including data pertaining to the telecommunications functions of dialing, routing, addressing or signaling, that identifies, or purports to identify, the origin, the direction, the time, the duration or size as appropriate, the destination or termination of a telecommunication transmission generated or received by means of the telecommunications facility owned by a service*



**Confidential**  
**Not for publication**

*provider (page 11).* The arbitrary separation of traffic data and content data is flawed. Traffic data has the potential to reveal as much about a person's private life as content data.

**Requirement to ensure intercept capability**

As mentioned above, we do not believe that service providers providing services outside the access remit of a traditional "ISP" would be required to ensure an intercept capability under the current wording of the draft provisions.

However, for traditional ISPs, the question remains as to what data categories an intercept capability would have to be maintained for. Is it the intention only to intercept emails (with or without content)? What about chat rooms, message/bulletin boards, newsgroups, web browsing? The longer the list, the greater the burden on industry and the greater the financial cost overall.

Finally, the consultation document does not provide details regarding proposed standards for technical requirements for the deployment of interception technology and as such does not provide a starting point for commenting on this issue as it relates to proposed regulations.

**Cost allocation when ensuring intercept capability**

We do not believe it right or just that service providers should be burdened with the cost of providing a lawful access intercept capability. Aside from the economic consequences of such a provision – which would be onerous, particularly for smaller service providers – there is no credible reason why business entities should pay for law enforcement activities. As the intercept activities carried out by law enforcement are supposedly in the public interest, it is reasonable to expect the costs to be borne by the public purse. This would also create a financial disincentive for law enforcement to conduct speculative (unnecessary, costly and intrusive) "fishing expeditions".

**Orders to obtain subscriber and/or service provider information**

It is unreasonable to expect service providers to collect personal subscriber information in addition to that which they already request for legitimate business purposes. Aside from the fact that business is not an extension of law enforcement (nor should it be used as such), there are serious concerns regarding the possible breaching of privacy laws. For example, and without limitation, a core principle (Principle #4) in Schedule 1 of the *Personal Information Protection and Electronic Documents Act* states that the collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. In addition, it states that organizations shall not collect personal information indiscriminately.

**Data preservation orders**

Given that the concept of data preservation does not exist in Canadian law, we would refer you to the submission of the government-appointed expert in this area, the Privacy

**Confidential**  
**Not for publication**

Commissioner of Canada. In the Commissioner's response to this consultation he states, "As the consultation paper indicates, the concept of a preservation order does not exist in Canadian law. This negates the argument that this type of authority is necessary to "maintain" existing lawful access capability." We see nothing in the consultation paper to contradict the Commissioner's view.

Were it to be clearly demonstrated by the government, however, that data preservation is an essential tool in fighting crime (convincing the Privacy Commissioner might be a good gauge of this), we would urge that the preservation period be as short as possible, for both business and privacy reasons. In a recent report the European Parliament recommended that data should be retained for no more than 30 days, without review. Indeed, the, as yet unratified by the Canadian Parliament, Council of Europe Cybercrime Convention – the pretext for this consultation – in Article 16 states "the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, ....". There is no suggestion, as there is in the consultation paper, that 120 or even 180 days preservation might be acceptable. In addition, preserving traffic data and e-mails for such a lengthy period of time for each user would require significant increases in storage facilities which would be costly to industry.

**Interception of e-mail**

As pointed out in the consultation document, there is no clear statement of the law regarding the legal status of e-mail. Yahoo! believes that the public generally believes that sending and receiving e-mail should be treated as a "private communication" as defined in Part VI of the *Criminal Code* and as such there should be a reasonable expectation of privacy. Accordingly, law enforcement would have to obtain judicial authorization to intercept. In addition, opened e-mails should receive the same protection as any other communication that is subject to search warrants or other legal orders.

**Other mechanisms to provide subscriber and service provider information**

While it might theoretically be possible for providers of paid for services, such as access services, to maintain full and reasonably accurate records of subscribers, it is not as simple for providers of free services. Many of Yahoo! Canada's services are provided free of charge. While we ask that users of certain services first register with us, we cannot compel them to provide us with wholly accurate information, or to provide a means of verification, such as a valid credit card number. Indeed, some users make use of the services precisely as it affords them a degree of legitimate anonymity.

It is difficult to see, therefore, how we could maintain a database of users for which we would be responsible for its "accuracy, completeness and currency". The privacy implications for the creation and maintenance of such a database, where the data is not needed for business reasons should also be considered. In addition, there is a concern

***Confidential***  
***Not for publication***

about security failures of the database and whether anyone other than law enforcement will have access to this database. The consultation document has not addressed safeguards the government is prepared to put in place to address these concerns.

We would add that no provision is made for such actions in the Council of Europe Cybercrime Convention, nor is this policy being pursued as far as we know by other Convention signatories.

In summary, therefore, no data should be demanded of users that is not needed for legitimate business purposes, no extra databases should be compiled for the same reason, and no central government-run database utilizing user data collected by service providers should be created.

**Conclusion**

In conclusion, we urge the Canadian government to conduct a fuller investigation into the areas where it believes current lawful access instruments to be insufficient, and in light of the results of that investigation, re-consider its proposals under consultation. It might be that there are indeed exceptional conditions under which law enforcement agencies could gain enhanced access to user and traffic data, but without a concrete demonstrated need, it appears hard to justify.

Should you have any further questions, please do not hesitate to contact us.

Yours faithfully,

s.19(1)



**Pierlot, Paul**

---

**From:** Document Control

**Sent:** 2002 Dec 16 3:55 PM

**To:** la-al@justice.gc.ca

Please find attached the submission of the Canadian Wireless Telecommunications Association regarding the Consultation on Lawful Access to Telecommunications. For more information, or clarification, please contact [REDACTED] Vice-President Industry & Regulatory Affairs, at (613) 233-4888 ext. [REDACTED]

s.19(1)

2002-12-18

000592

## **Lawful Access Consultation**

### **Response of the Canadian Wireless Telecommunications Association**

**submitted to  
Department of Justice  
Industry Canada  
and  
Solicitor General Canada**

**December 16, 2002**

## **Introduction**

1. The Canadian Wireless Telecommunications Association ("CWTA") has carefully reviewed the Lawful Access Consultation Document (Consultation Document), issued by the Department of Justice, Industry Canada and the Solicitor General Canada on August 25, 2002.
2. CWTA is the authority on wireless issues, developments and trends in Canada. It represents cellular, PCS, messaging, mobile radio, fixed wireless and mobile satellite carriers as well as companies that develop and produce products and services for the industry.
3. This response to the Consultation Document contains an overview of the key issues identified by the CWTA and several sections organized to mirror the sections contained in the Consultation Document followed by a Conclusion.

## **Overview**

4. The CWTA recognizes that lawful access is an important tool for national security and law enforcement. The services provided by wireless carriers also serve important objectives of federal telecommunications policy. The CWTA understands that the impetus behind the review of the legislative framework for the provision of lawful access to communications is tied to the Council of Europe Cybercrime Convention.
5. We would like to provide constructive comments regarding the proposal but our ability to do so is limited at this time. While the Consultation Document provides a somewhat helpful high-level overview of the issues at hand, a number of critical questions remain unanswered regarding the proposals contained in the document. In order to provide meaningful comment on the policy proposals, service providers must understand the requirements that they will be expected to meet under the new legislation. These detailed requirements are not included in the Consultation Document.
6. In a letter to the Minister of Justice dated November 1, 2002; CWTA requested that draft legislation as well as any accompanying regulations be provided for public consultation. After further review of the Consultation Document and the issues, CWTA is now of the view that a further round of consultation is warranted.
7. The CWTA strongly suggests, therefore, that prior to any draft legislation being presented to Parliament, the Departments should provide a second

public consultation paper containing the details absent from the current document. The CWTA and its members need to better understand the entire operational framework of the lawful access proposal.

8. The entire operational framework will, of necessity, be very complex. It will impact several Acts of Parliament and will involve all three levels of government. Only after the entire framework is understood will the CWTA be able to ascertain all of the various impacts that the proposed legislation will have on the wireless telecommunications industry. In this regard, the CWTA notes that the submission of the Privacy Commissioner of Canada repeatedly expresses concern over the lack of critical details in the Consultation Document.
9. The CWTA also proposes that the new requirements not take effect immediately on the day the new legislation comes into force. A period of time will be required during which service providers and vendors alike will come to fully understand the new requirements and enable the service providers to make the required network modifications to meet the basic intercept capability. It is the view of the Association that the suggested grace period is a very positive and pragmatic proposal. None of the stakeholders to the lawful access initiative, including law enforcement, government, service providers nor Canadian citizens, would benefit from the introduction of new and immediate requirements if the technology to meet the new requirements is unavailable.
10. Moreover, as indicated in the Consultation Document, much of the impetus for the proposed legislation stems from the Council of Europe Convention on Cybercrime. The CWTA understands that the European Community itself continues to develop specific regulations. Accordingly, it would be prudent for Canada to undertake a further consultation once the details of the European regulations are known.
11. A number of elements within the current proposal may have significant impacts on the manner in which wireless carriers conduct their business and may significantly increase the cost of doing so. The CWTA is opposed to any new obligations, such as validation of customer information, that would require a radical and costly overhaul of wireless carrier business processes and services. CWTA is also opposed to any obligation that might cause the elimination of certain services or class of services, such as prepaid wireless. Law enforcement and security interests must be fairly balanced with the interests of the communications industry and wireless consumers.
12. A transparent process is required that would clearly articulate the requirements for compliance that must be met by all carriers. All service providers competing in the same market should face the same

requirements to provide the same level of lawful access to communications. At the same time, regulations or standards must be flexible enough to accommodate the different technologies employed by wireless carriers.

13. Significant hardware systems and software upgrades may be required in order to comply with any new lawful access standards that may result from the passage of new legislation. The CWTA is opposed to the imposition of proprietary or uniquely Canadian solutions for lawful access. Where new standards are developed, the CWTA strongly endorses the harmonization of such standards with international telecommunications industry standards. An industry standard approach would increase the likelihood that technology vendors will develop and provide technology that satisfies the lawful access requirements. This approach would also likely result in costs that are lower than would be the case if proprietary solutions are required. CWTA notes that these standards will largely be driven by the markets in the United States and Western Europe, areas that are also moving to ratify the Convention on Cybercrime.
14. The new legislative framework must recognize that the benefits associated with lawful access accrue to all Canadians and therefore it is Government that must provide the financial resources to pay for the network modifications necessary to meet the lawful access requirements. Regardless of whether or not retrofitting is required, the tools and equipment to provide lawful access will represent a significant incremental cost to industry; one that industry cannot bear alone. Moreover, any future modifications of the standard would require additional financial commitment by the government.
15. The final concern to be emphasised in this overview pertains to service provider liability in the provision of lawful access. The CWTA is of the view that the new law must not leave service providers open to legal actions by customers or others for the mere provision of lawful access. Accordingly, the new legislation should provide appropriate safe harbour liability protection provisions for service providers.

### **Current Provision of Lawful Access**

16. As noted in the introduction to the Consultation Document, certain providers of wireless services have been required to have facilities capable of lawful access pursuant to conditions of licence imposed under the *Radiocommunications Act*. Contrary to the apparent view of some law enforcement / government stakeholders, however, the lawful access proposal will nonetheless impose significant new obligations on wireless carriers with respect to packet-switched services. While the current



conditions of licence do not detail the specific obligations of wireless carriers, the conditions do require that carriers adhere to the requirements of the Solicitor General. The Solicitor General has, in turn, developed a document that outlines the enforcement standards for lawful interception of telecommunications (often referred to as the Solicitor General's 23 Standards).

17. The 23 Standards were developed in an era of circuit-based switching and can only reasonably be interpreted to apply to services offered using circuit-based switching. The CWTA strongly disagrees with any and all assertions that the Solicitor General's 23 Standards apply to services offered using packet-based switching. Various policy documents from the Department of Industry provide reference for CWTA's position:
  - a. PCS Spectrum Licence Condition 11 states "Licensees using the spectrum for circuit-switched voice telephony systems must, from the inception of service, provide for and maintain lawful interception capabilities as authorized by law".
  - b. *The Policy & Licensing Procedures for the Auction of Additional PCS Spectrum in the 2 GHz Frequency Range* (DGRB-005-00/DGTP-007-00, June 2000) states "The Department notes that the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications were written to apply to circuit-switched voice telephony systems and as such, the standards are not readily applicable to a packet-based environment using routers rather than traditional switches...the Department will only incorporate compliance with the Solicitor General's current standard for circuit-switched voice telephony systems."
  - c. In the Policy and Licensing Procedures of both MCS at 2500 MHz (DGRB-006-99) and the Auction of the 24 and 38 GHz Frequency Bands (DGRB-003-99/DGTP-005-99) the Department chose not to "incorporate compliance with the Solicitor General's current standard into a licence condition at this time" because the services were not anticipated to provide circuit-switched voice applications.
18. Further, it is unclear, in our view, as to what will happen to the existing conditions of licence and the Solicitor General's 23 Standards once new legislation is passed. The CWTA would assume that the new laws would take precedence over the current licensing conditions and would assume further that new regulations would be passed which would be linked directly to the new law.
19. It must also be emphasised that wireless carriers operate a variety of networks using different technologies. These networks are also at various

stages of development and deployment. In this regard, while the Consultation Document suggests that wireless carriers already provide lawful access; in reality not all wireless carriers are at the same level of compliance with the Solicitor General's 23 Standards. The question therefore arises as to whether the relevant state of compliance with the 23 Standards will be entrenched with the new law?

20. The CWTA therefore recommends that existing conditions of licence pertaining to the provision of lawful access be rescinded once the new law is in force. CWTA further recommends that all forbearance conditions currently in-place, should be continued over and remain in force for a reasonable period under the new legislation.
21. The CWTA is strongly of the view that it is the responsibility of Government to pay for all costs associated with the provision of lawful access. If the Government accepts this responsibility, then the need to maintain the existing forbearance decisions will become moot. In addition, the use of Government resources will enable the application of identical requirements to all carriers in a timely and consistent manner.
22. The Solicitor General's 23 Standards and, as a result, the interception capabilities of wireless carriers, deal primarily with the interception of circuit-switched voice and data received or transmitted by a wireless customer. As indicated above, the CWTA is strongly of the view that the Solicitor General's 23 Standards can only be legitimately applied to services offered using circuit-based switching. The Consultation Document, however, with its strong linkages to the European Convention on Cybercrime, suggests a number of requirements pertaining to the Internet that are not detailed in the 23 Standards. As such, the CWTA would anticipate that this aspect of the new law would have a significant impact on the wireless industry. Most wireless carriers offer services and sell devices that will allow customers to send and receive email, as well as browse the Internet over packet-based networks.
23. The CWTA further notes that the Consultation Document alludes to tools such as data retention, prevention of virus dissemination and subscriber and service provider information. These mechanisms are not found in the Solicitor General's 23 Standards and, as such, would have a significant impact on the wireless industry. These impacts are detailed later in this response.
24. The CWTA is opposed to the imposition of requirements that will significantly impact existing services, distribution channels and business processes. These things have been developed by wireless carriers for business purposes including the provision of services, and the collection of revenues. Any information or data that is incidental to these purposes

may or may not be useful to law enforcement and security agencies. The CWTA is not opposed to making such information available in the context of lawful access. However, it is opposed to the notion that carriers will be required to undertake substantial modifications, or to eliminate certain distribution channels or services in order to comply with new lawful access requirements.

## Working Definitions

25. The Consultation Document introduces a number of working definitions including "Service Provider", "Transmission Facility", "Transmission Apparatus" and "Telecommunications Associated Data". CWTA is concerned that other fundamental terms such as "Basic Intercept Capability" and "Significant Upgrade" are not defined in the Consultation Document.
26. At the outset the CWTA would note that the definitions provided differ from those provided by the *Telecommunications Act*. In particular, the *Telecommunications Act* contains definitions of "Telecommunications Facility", "Transmission Facility" and "Telecommunications Service" (as opposed to "Service Provider"). A definition of "Telecommunications" is also provided.
27. Confusion could arise from two Acts containing differing definitions. The CWTA recommends that the new law use, where possible, existing definitions contained in the *Telecommunications Act*.
28. In addition, the working definition provided in the Consultation Document for service provider is given as: "means a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada". This definition omits an entire class of service providers referred to as "resellers", and also would appear to exclude entities such as technology vendors, enhanced service providers, and application service providers, any of which may own and operate computer servers and/or systems that form an integral part of the services they provide to other service providers such as wireless carriers. Wireless carriers cannot be held liable for data, servers and systems that they do not control.
29. In this regard, the language used in the European Convention may be helpful, "any public or private entity that provides to users of its service the ability to communicate by means of a computer system", and "any other entity that processes or stores computer data on behalf of such communication service or users of such service."

30. While in our view the definition of service providers omits several classes of providers, it does appear to capture a number of smaller organizations like hotels, universities and, possibly, coffee shops that operate a transmission facility and offer service to the public. It is also our understanding that some types of service providers might somehow be exempted from complying with the obligation to provide intercept capabilities. Such exemptions, if they materialize, would obviously be a concern from the standpoint of public security but also from standpoint of creating a level playing field for competitors in the communications industry. It would be unjust to require larger licensed service providers to fully comply with the new legislation while exempting smaller competitors from compliance with the new legislation. The CWTA submits that all service providers competing in the same market should face the same requirements to provide the same level of lawful access to communications.
31. The working definition of Telecommunications Associated Data is "means any data, including data pertaining to the telecommunications functions of dialling, routing, addressing or signalling, that identifies, or purports to identify, the origin, the direction, the time, the duration or size as appropriate, the destination or termination of a telecommunication transmission generated or received by means of the telecommunications facility owned or operated by a service provider." It is unclear from this definition whether wireless carriers would be expected to provide the specific location of the customer (assuming location information is available) and whether the carrier would be further expected to update (track) the location information. CWTA notes the Privacy Commissioner of Canada expressed some concern about this idea.
32. The CWTA agrees with the working definitions of Transmission Facility and Transmission apparatus.

### **Specific Legislative Proposals**

33. The following section addresses the specific proposals contained in the Consultation Document as they are presented in the document.

### ***General Requirements***

34. As noted earlier, CWTA is extremely concerned that the concepts of "Basic Intercept Capability" and "Significant Upgrade" are not defined in the Consultation Document. This makes it most difficult to provide meaningful comment as to the appropriateness of these concepts.

35. This concern is most pronounced when considered in light of the proposal that service providers would be expected to cover the costs associated with these proposals. If sufficient funding is available from government, the potential impacts of these definitions would be less severe.
36. Nevertheless, the CWTA believes that the mere extension of service areas should not be considered as a significantly upgraded service to the public. Wireless carriers are continually extending the coverage areas of their networks to better serve their customers. These incremental additions, even where they may be geographically broad, do not change the characteristics of the services available but merely allow access to services in areas previously un-served.
37. "Significant upgrade" should be defined as being the replacement of, or substantial modification to, the entire hardware and software platform utilized by the service provider's core network.
38. "Core network" should be defined as the physical entities which provide support for the network features and telecommunication services. The support provided includes functionality such as the management of user location information, control of network features and services, the transfer (switching and transmission) mechanisms for signalling and for user generated information.
39. It is worth noting that, whatever the definition, network equipment must be available to provide the capability. The CWTA therefore believes that the date that the requirements of the legislation would come into effect, as proclaimed by the Governor-in-Council, should be a minimum of 12 months after the new legislation comes into force. A period of time will be required during which service providers and vendors alike will come to fully understand the new requirements and enable the service providers to make the required network modifications to meet the basic intercept capability. It is the view of the Association that the suggested grace period is a very positive and pragmatic proposal.

### ***Regulations***

40. As noted above, some wireless carriers have experience in providing lawful access to communications. Some of the challenges these carriers faced in the provision of lawful access relate to the regulation-like standards developed by the Solicitor General. The interpretation of these standards has, in some respects, evolved since the conditions of licence were first imposed – causing the wireless carriers to modify their networks and operational procedures in order to remain in compliance with the evolving requirements.

41. The CWTA supports the creation of specific regulations or standards that clearly define what must be done. However, the regulations or standards must be flexible enough to accommodate the different technologies employed by wireless carriers.
42. Moreover, it is the view of the CWTA that the new regulations should not be modified without consultation with industry and without consideration of the cost impact on industry associated with changing the regulations. Additional impacts can occur after changes to regulations if law enforcement agencies don't all modify their own systems, forcing service providers to provide data in more than one format or mode. The regulations should also require law enforcement agencies to upgrade their equipment to accommodate any jointly agreed modifications to standards or methods.
43. While the Consultation Document speaks to adoption of new technologies by service providers, it does not speak to the impact of changes in regulations. Costs associated with changes to the regulations should be the responsibility of government, not industry.
44. The CWTA would further urge that the regulations be consistent with international telecommunications industry standards. This would help to reduce the costs associated with the provision of lawful access. The CWTA is opposed to the notion that proprietary or uniquely Canadian solutions will be imposed on wireless carriers.
45. With regard to fees for the ongoing provision of lawful access, the CWTA is of the view that it is appropriate for carriers to charge fees for the provision of lawful access service. This would be consistent with the approach taken by other jurisdictions.

#### *Forbearance*

46. As noted in our comments regarding the definition of service provider, we understand that some types of service providers might somehow be exempted from complying with the obligation to provide intercept capabilities. Such exemptions, if they materialize, would obviously be a concern from the standpoint of public security but also from standpoint of creating a level playing field for competitors in the communications industry. It would be unjust to require larger licensed service providers to fully comply with the new legislation while exempting smaller competitors from compliance with the new legislation.

47. CWTA cannot provide detailed comments on this issue as the concept of exemption is not included in the Consultation Document, and no details have been provided regarding any process that may be used to determine an exemption. The CWTA submits that all service providers competing in the same market should face the same requirements to provide the same level of lawful access to communications.
48. As in the comments on the definitions of "Basic Intercept Capability" and "Significant Upgrade", the concern about ensuring equitable obligations between competitors is most pronounced when considered in light of the proposal that service providers would be expected to cover the costs associated with these proposals. If sufficient funding is available from Government, the market distortions from such exemptions will be minimized.
49. The CWTA believes that any service provider that is unable to meet the basic minimum intercept requirements should be required to seek forbearance.
50. The CWTA supports the proposal that a forbearance mechanism be included in any new scheme.
51. The CWTA wishes to emphasise the importance of a fair and open public process dealing with all requests for forbearance.

#### ***Compliance Mechanism***

52. The CWTA believes a complaint driven compliance mechanism in which the law enforcement agencies would most likely be the complainant, is the most suitable approach.
53. Given the technical nature of the provision of lawful access service, the CWTA is of the view that the Minister of Industry, through his Department, is the appropriate delegate to determine compliance.
54. The CWTA believes that wireless carriers are currently meeting what will become the basic intercept capability in the new legislation. If it is deemed that a service provider is not meeting this basic capability, then it would be appropriate for the service provider to seek forbearance.
55. If forbearance is not granted and prior to the imposition of any penalty, the CWTA strongly believes that service providers should be afforded with a period of time in which to transition from non-compliant state, to a state of compliance. The CWTA recommends a transition period of 12 months.

### ***Costs of Ensuring Intercept Capability***

56. Significant hardware and software systems may be required in order to comply with any new lawful access standards that may be developed. The CWTA fully supports an approach whereby new requirements are harmonized with industry standards. This will increase the likelihood that solutions will be made available by a broad range of vendors, and will likely result in lower cost than would be the case for proprietary solutions.
57. The benefits associated with lawful access accrue to all Canadian citizens and therefore it is Government that must provide the financial resources to pay for the network modifications required to meet the lawful access standard, as is the case with other policing and national security costs. Moreover, any future modifications of the standard would require additional financial commitment by the government.
58. The Consultation Paper proposes the following regime governing costs:
  - a. *Service providers would be responsible for the costs associated with providing the lawful access capability for new technologies and services, and*
  - b. *Service providers would be responsible for the costs associated with providing a lawful access capability when a significant upgrade is made to their systems or networks, however*
  - c. *They would not be required to pay for necessary changes to their existing systems or networks.*
59. It would appear that the Departments have proposed this cost regime based on the following assumptions:
  - a. that the cost of retroactively-fitting existing systems or networks to provide new lawful access capabilities will be substantial,
  - b. that, in comparison to the cost of retro-fits, the cost of incorporating new capabilities into the design of a new system or network from the beginning are usually lower, and
  - c. that the costs of incorporating new capabilities into the design of a new system or network, or into a "significantly upgraded" service, are not substantial and are insignificant.
60. CWTA agrees with the assumption that in general, costs associated with retro-fits are significant. CWTA submits however, that although lower than the costs of retrofitting, the costs of incorporating capabilities into new



systems and networks are also significant. Even when services and capabilities are included in a standard package, significant software activation charges must often be paid to the vendor before that service or capability can be activated. Only in time will the cost of incorporating lawful access services or capabilities into new systems or networks become relatively insignificant and therefore will no longer require the application of explicit charges.

61. CWTA submits that service providers should only be responsible for the cost of providing lawful access capabilities in new systems or networks, or in significantly upgraded services, when the cost of doing so is no longer significant and is implicit in the cost of the basic feature package. In other words, public funding should be provided as long as the cost of providing lawful access for existing, significantly upgraded, or new services and networks is significant, and as long as the capabilities in question are only available upon payment of explicit charges.
62. With regard to the ongoing provision of lawful access service to law enforcement agencies, the CWTA believes that the new legislation should enshrine the principle that law enforcement should pay service providers for assistance provided. While the federal law enforcement agencies generally accept this principle, some CWTA members have experienced difficulty recovering their costs in providing the required service to certain local law enforcement agencies.
63. The provision of lawful access services to law enforcement goes well beyond the concept of civic duty on the part of service providers. Providing assistance to law enforcement agencies generates significant ongoing costs in terms of personnel, training, and security requirements in addition to the specific costs of implementing an interception capability.
64. It is the view of the CWTA that an enshrined principle would assist both service providers and law enforcement agencies to arrive at negotiated fee for service arrangements with each other.
65. The CWTA further believes that, in addition to enshrining the principle described above, the legislation should point to the Departments of Industry Canada and Solicitor General as arbitrators to any dispute regarding fee for service between a service provider and a law enforcement agency.

## **Amendments to the Criminal Code and other statutes**

### ***Orders to obtain subscriber and/or service provider information***

66. The CWTA strongly opposes the imposition of this obligation beyond those situations where a wireless carrier is already collecting this information. Moreover, the CWTA is of the view that service providers should not be liable for the accuracy of customer name and/or address information. In this regard, the CWTA would note that the European Convention refers to subscriber information *in that service provider's possession or control*.
67. Generally, wireless carriers collect, validate and maintain customer information to the extent that such information is necessary to successfully provide service and to collect payment. For postpaid services (services for which the customer receives a monthly bill), wireless carriers would typically undertake a credit check to determine a prospective customer's ability to make monthly payments for the services provided. However, this process is geared to validating credit worthiness, not customer name and address. Wireless carriers do not undertake exhaustive validation of the information that is provided by customers and wireless carriers do not warrant that such information is valid or correct, or that it would satisfy the requirements of law enforcement and security agencies. Further, wireless carriers are almost entirely reliant on customer initiated notification with respect to address changes.
68. Consequently, the CWTA opposes the imposition of any obligation for service providers to collect information that they are not already collecting for their own purposes. Significant service, business and cost issues would arise if wireless carriers were required to collect, validate and maintain accurate customer information for the purposes of lawful access.
69. First, any such requirement would likely obligate wireless carriers to insist that customers present a minimum degree of official identification at the point of purchase. This would also require that wireless carriers, and the literally thousands of independent distribution agents and outlets they rely on, would be capable of validating such identification. CWTA notes in this regard the concerns raised by the Privacy Commissioner of Canada.
70. Second, an overwhelming issue arises with respect to on-line purchases of a wireless service since, for these purchases, the entire transaction is conducted over the Internet, not in person. Similarly, customers who opt for on-line billing will be billed on-line and will not have a monthly invoice sent to a physical address. If they chose to move, the carrier will have no

means of knowing, apart from the customer taking the initiative to update this information by accessing their on-line account. In the case of purchasing or billing, on-line transactions do not lend themselves to the presentation and validation of the customer's identification. Wireless carriers, and countless other businesses in Canada and abroad, have already made significant investments in on-line purchasing, billing and customer relations capabilities and they rely on this channel as a useful and cost-effective means by which to acquire, bill and interface with their customers.

71. Third, another problem is created with respect to prepaid wireless services provided by wireless carriers since valid customer information is not required by carriers in order to provide prepaid services. Given that a credit check is not required, and that the customer will never receive a monthly bill, there is no need for the carrier to request the customer's name or address. The entire transaction of activating the customer's account can be conducted over the phone and absent any identification. Although wireless carriers are increasingly requesting customer name and address information for business purposes, this information is not validated, nor do carriers deny service if the customer does not provide the information.
72. It should be noted that this situation is not isolated to wireless phones. The verification of a customer's address is only necessary when a service provider must establish a physical connection to the customer. For example; Direct Broadcast Satellite, Multipoint Distribution Service, dial-up Internet Service Providers, and prepaid local and long distance phone card providers are also capable of providing service without knowing the address of the customer.

### *Assistance Orders*

73. As noted earlier, CWTA believes that the new legislation should enshrine the principle that law enforcement should pay service providers for assistance provided. While the federal law enforcement agencies generally accept this principle, some CWTA members have experienced difficulty recovering their costs in providing the required service to certain local law enforcement agencies.
74. It is the view of the CWTA that an enshrined principle would assist both service providers and law enforcement agencies to arrive at negotiated fee for service arrangements with each other.
75. The CWTA further believes that, in addition to enshrining the principle described above, the legislation should point to the dual Departments of

Industry Canada and Solicitor General as arbitrators to any dispute regarding fee for service between a service provider and a law enforcement agency.

***Data-preservation orders***

76. The CWTA would note that this is another area of the Consultation Document that would benefit from the inclusion of more details. We currently understand that data-preservation in this context means a snapshot of data that a service provider has access to at a point in time. Moreover the order would only apply to data that service providers would ordinarily save during their normal course of business.
77. The CWTA wishes to emphasise that it would be extremely unreasonable to expect service providers to immediately comply with a data-preservation order as soon as the order is served on the service provider. While every effort would be made to expedite compliance with the order, such compliance would not be instantaneous.
78. It is also our understanding that the data-preservation order should only apply to computer data.
79. The CWTA believes that only the courts should be authorized to issue a preservation order.
80. The CWTA recommends that the custodian of data should not be compelled to preserve data any longer than is absolutely necessary. The operational and storage costs associated with preserving data are high. In consultations, the Departments indicated that the majority of data-preservation orders would require that data be preserved only for 2-3 days while the maximum 90 day period mentioned in the Consultation Document would only be required in those cases that require international cooperation. CWTA suggests that the text of the legislation should indicate a shorter "typical" application, while allowing for a longer maximum for international cases.

**Other mechanisms to provide subscriber and service provider information**

81. CWTA is not convinced that any new mechanism for law enforcement to identify a local service provider is required.
82. The CWTA notes that the Canadian Numbering Administration Consortium Inc. (CNAC) will, in part, respond to these stated needs of law enforcement to link a telephone number to its service provider. As directed

by CNAC, the Canadian Numbering Administrator provides on its website (<http://www.cnac.ca/>) a listing of NPA-NXX combinations along with the name of the code holder (almost always the service provider) for each. For example, 613-728 is a NPA-NXX combination used in Ottawa-Carleton to provide local telephone service and the code holder is Bell Canada. Anyone who wishes to consult the website is able to freely identify the service provider. This is referred to as the National Numbering Index, or NNI. It is also worth noting that this information is already publicly available, for a cost, from the Telcordia NPA/NXX database.

83. The CWTA also notes that there is an existing Bell Canada tariff which allows law enforcement agencies, under CRTC specified conditions, to access an enhanced NNI which also reflects the impacts of local number portability and can therefore provide the service provider for each line number NPA-NXX-XXXX in the country.
84. The CWTA is extremely concerned about the costs and practicality of creating another mechanism to maintain up-to-date and accurate CNA and LSPID information.
85. For certain services, wireless carriers do not collect CNA information for their own purpose. Any requirement to do so would impose additional costs on wireless carriers. The CWTA is concerned with the legal ramification of forcing service providers to be gate keepers of CNA information and the implication that service providers should somehow be accountable for the accuracy of said information.

### Liability Issues

86. The CWTA is of the view that service providers must not be open to civil or criminal liability for any actions taken pursuant to the new law. Accordingly, the new legislation should provide appropriate safe harbour liability protection provisions for service providers. This would be consistent with the actions of other jurisdictions. The text from the New Zealand *Telecommunications (Interception Capability) Bill 2002* provides an example of liability protection clause: "Every network operator, service provider, surveillance agency and person employed or engaged by any such operator, provider or agency is protected from liability for any act done or omitted to be done in good faith under this Bill".
87. The CWTA notes that situations have arisen (in the US) whereby the account of a mobile phone being used for illegal activities lapses into default and the service was disconnected. This has jeopardised the police surveillance. In such a situation the CWTA believes the carrier should not be held liable. Moreover, if the account is not being paid by the individual under surveillance, then the costs of maintaining the account — if required

for law enforcement purposes — should become the financial responsibility of the law enforcement agency.

88. In the situation described above and where the wireless device in question has been stolen, an additional issue arises — namely control over the phone number. Ordinarily, the stolen handset would be denied service and the rightful owner of the handset would retain his or her phone number using a new device. In such circumstances, wireless carriers must be permitted to reinstate service to the rightful account owner.
89. While some would argue that the Criminal Code provides blanket limitations on liability, it is unclear that these limitations also extend to civil matters. Moreover, it is unclear on how the blanket limitations would extend to obligations that might exist in a new law. As a result, CWTA urges the Departments to ensure that adequate safe harbour provisions are included in the new legislation.

## **Conclusion**

90. CWTA recognizes the importance of lawful access to communications by law enforcement in Canada and appreciates the opportunity to provide these general comments on the Consultation Document. Again, CWTA notes that a number of critical questions remain unanswered regarding the proposals contained in the document. CWTA is of the view that further consultation on the details absent from the current document as well as full consultation on proposed legislation and accompanying regulations and standards, is still required.
91. Notwithstanding the above, CWTA believes that the following actions must be taken in the upcoming legislative proposals:
  - a. Make available sufficient federal funding for service providers:
    - i. to retrofit all networks and systems to satisfy all lawful access needs of law enforcement authorities (LEAs) ;
    - ii. to cover all incremental costs to provide the capability for lawful access to new networks and systems providing upgraded, significantly enhanced and new services; and
    - iii. to pay service providers, as necessary, for their operational costs to provide all lawful access services that may be requested by local, regional and national law enforcement agencies.
  - b. The principle that law enforcement should pay service providers for assistance provided must be enshrined in the new legislation.

c. Address specific issues for licenced wireless carriers

- i. The proposals in the Consultation Document go beyond the current requirements imposed on wireless carriers for interception of circuit switched services. It is anticipated that these new obligations will significantly impact wireless carriers.
- ii. Existing Conditions of Licence for wireless carriers pertaining to the provision of lawful access should be rescinded once the new law is in force.

d. Ensure definitions are appropriate

- i. Clear definitions of the terms "Basic Intercept Capability" and "Significant Upgrade" must be established.
- ii. The definitions proposed in the Consultation Document should align with those of the *Telecommunications Act* as much as possible.
- iii. The definition of "Service Provider" should align more closely with the language of the European Convention to include "any public or private entity that provides to users of its service the ability to communicate by means of a computer system", and "any other entity that processes or stores computer data on behalf of such communication service or users of such service." This definition must also ensure that all competitors in the same market face the same obligations.

e. Provide for an efficient transition between regimes

- i. A transition period of at least 12 months must be provided from the enactment of the legislation to provide service providers and equipment vendors the time to understand and meet the requirements.
- ii. Forbearance decisions should be made in a fair and open process.

f. Ensure existing business processes are not unduly impacted

- i. Any requirement to provide subscriber information should be limited to that in the service provider's possession or control.
- ii. There must not be any obligation to validate customer information.
- iii. There is no need for an additional mechanism to provide LSPID to law enforcement agencies.

**g. Provide adequate liability protection for service providers**

- i. Service providers must be afforded protection from civil and criminal liability for activities related to providing lawful access. As such, new legislation should provide appropriate safe harbour liability protection provisions for service providers.**



Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 16 4:09 PM  
To: la-al@justice.gc.ca  
Subject: Comments on the Lawful Access consultation document



privaterra\_la.pdf

To Whom It May Concern:

Please find attached as an Adobe PDF file, a joint submission by the Privaterra Project and Computer Professionals for Social Responsibility on the Lawful Access Consultation document.

Thank you for the opportunity to participate in this process. Speaking for Privaterra/CPSR and, I suspect, all other Canadian civil society members, I hope this is merely the beginning of a dialogue on this issue and not the end of the conversation.

Of course, I would be happy to clarify or expound on any point made herein, should the Government so require.

Sincerely,

[REDACTED]  
Director,  
Privaterra

--

---

<http://www.lexinformatica.org>  
<http://www.privaterra.org>  
<http://www.epic.org>  
PGP KeyID 0x46E11518

**Comments submitted to the Departments of Justice, the  
Solicitor-General and Industry Canada in consideration  
of the Council of Europe *Convention on Cyber-crime*  
and the Lawful Access Consultation Document**

**Privaterra**

A Project of Computer Professionals for Social Responsibility

November 21, 2002

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

## **Executive Summary**

The Canadian government's *Lawful Access* discussion paper fails to provide empirical – or anything beyond anecdotal – evidence that the legislative amendments proposed are actually needed. Evidence derived from U.S. law enforcement agencies suggests that technological and administrative impediments – more than legal ones – are the cause of most difficulties experienced in cybercrime investigations and prosecutions, specifically: insufficient basic record keeping by telecommunications and Internet service providers; inability to effect data preservation extraterritorially; inability to circumvent encryption; and, a lack of common data-sharing protocols.

Under the guise of international obligations, the government seeks to adopt new legal investigatory tools, the effect of which would be a dilution of judicial oversight for the production of digital "traffic data" in criminal investigations. Unlike the analog analogue, digital traffic data will often reveal a great deal about one's lifestyle, intimate relations or political or religious opinions. Canadian courts have unequivocally found that information of this nature is subject to the highest constitutional protections, particularly in the criminal investigation context.

The *Lawful Access* consultation paper misinterprets the Supreme Court's standard for finding a 'reasonable expectation of privacy', by failing to distinguish between the nature of information contained in the various categories of traffic and the label "traffic data", which is otherwise legally meaningless. 'Traffic data' should attract a reasonable expectation of privacy under the *Plant* doctrine if it passes within the permeable walls of the biographical core or, under the *Shearing* and *Law* doctrines, if the owner of the information held a subjective reasonable expectation of privacy in the data, regardless of its content.

By their nature, packet-mode communication intercepts are liable for massive infringement of third-party *Charter* rights, which the Supreme Court held in *Thompson* can be determinative of constitutionality. Further, investigatory tools for packet-mode communications cannot separate traffic and content data, necessitating a high reasonable expectation of privacy standard for both.

The government's discussion paper claims that production orders – executed by third-party telecommunications or Internet service providers – would be less invasive than traditional search warrants. This arguments overemphasizes the physical aspect of a search and fails to recognize that s. 8 of the *Charter of Rights and Freedoms* protects people, not places or things against unreasonable search and seizures.

The history of investigatory detentions under highway safety legislation shows that subjectively-based assessments can too easily mask discriminatory conduct by law enforcement. Contrary to popular understanding, discrimination is a corollary of discretion, not a synonym for racism. It is not a 'dirty word', but simply an accepted condition that must be factored into the administration of the law. Diluted judicial

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on  
Lawful Access*

oversight in the context of cybercrime investigations expands law enforcement and third-party discretion to discriminate and could lead to the *de facto* offences of, for example, "surfing while Muslim", or of being political, a teenager, or belonging to a negatively-stereotyped group in cyberspace.

Applying traditional rules of lawful access to the persistent, pervasive and permanent information realm of cyberspace introduces new and unique implications for privacy and freedom of expression. The efficacy of electronic surveillance is such that it has the potential to annihilate any expectation that our communications will remain private. A society which exposes us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we send an email or visit a web site might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. Consequently, proposed legal 'solutions' to what are often technological or administrative dilemmas may not be the most equitable approach for extending effective policing and intelligence authority to cyberspace. To the extent that governments choose legal tools to investigate and prosecute 'cybercrimes', great care must be taken that they do not abrogate existing constitutional protections.

**Who are the authors?<sup>1</sup>**

*What is the Privaterra Project?*

A project of Computer Professionals For Social Responsibility (CPSR), a U.S. 501(c)(3) non-profit, charitable institution, Privaterra provides information privacy and security technology, education and support for human rights workers worldwide.

Drawing on the expertise of some of the world's leading computer professionals, cryptographers, legal experts and established human rights organizations, Privaterra seeks to educate human rights workers about the vulnerabilities inherent in new information and communications technologies and to provide information privacy and security tools to assist them in carrying out their important missions.

Privaterra has offices in Toronto, Ontario, Palo Alto, California and Lima, Peru. More information on Privaterra and its activities can be found on its website at [www.privaterra.org](http://www.privaterra.org).

s.19(1)

Project. He gratefully acknowledges the assistance of the Hon. Justice

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

### *What is the Computer Professionals for Social Responsibility?*

Founded in California in 1981, Computer Professionals for Social Responsibility (CPSR) is a public interest alliance of computer scientists and civil rights activists concerned about the impact of computer technology on the public. As technical experts, CPSR members provide the public and policymakers with realistic assessments of the power, promise, and limitations of computer technology. As concerned citizens, CPSR directs public attention to critical choices concerning the applications of computing and how those choices affect society. More information on CPSR and its activities can be found on the CPSR website at [www.cpsr.org](http://www.cpsr.org).

### **Introduction**

On 28 August 2002, the Department of Justice, Solicitor-General and Industry Canada issued a public consultation document proposing amendments to several important federal statutes, including the *Criminal Code*.

Among other measures, the proposal seeks to introduce several new investigatory powers which would grant law enforcement, regulatory and national security agencies access to telecommunications and Internet service provider ("ISP") subscriber and "traffic data", under a lesser standard than that now required for search warrants.

The *Criminal Code* and other statutes generally provide that state agencies cannot obtain documents or information without first establishing a factual foundation of 'reasonable and probable' grounds that an offence has been or will be committed. This requirement serves two purposes: first, it is a check against the unfettered discretion of law enforcement to look for and collect evidence of crime at the expense of individuals' *Charter* rights; and, second, it creates a record of accountability subject to audit of abuse of authority and defects in the law.

This discussion begins with reference to some of the impediments faced by law enforcement in the investigation and prosecution of 'cybercrime'. The paper next addresses the question of what are Canada's obligations under the Council of Europe's *Convention on Cyber-crime*, on the assumption that the government will ratify the treaty. A brief article-by-article review of the substantive law requirements of the convention precedes an issues-based analysis of the proposed procedural amendments, the only amendments substantially reflected in the government's *Lawful Access* document.

Appendix A of this document contains examples of the nature of information found in various types of "traffic data", underlining the importance of a contextual approach when considering its legal status.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

**What are the impediments to the investigations of cybercrime that the lawful access initiative seeks to address?**

*The Lawful Access document does not provide sufficient background for proper assessment of impediments to the effective investigation of cybercrimes.*

s.19(1)

A foundation criticism of the *Lawful Access* document<sup>2</sup> and consultation must be the lack of empirical – or anything beyond anecdotal – evidence that the legislative amendments proposed are actually needed.<sup>3</sup> As [redacted] commented: "[T]he proposal merely points to the need to comply with the cybercrime treaty as the primary rationale for many of the reforms."<sup>4</sup> This observation was repeated by individuals at the civil society consultations held in Ottawa, Montreal and Vancouver.

At the Ottawa roundtable, the Department of Justice presented a slide showing that applications for authorization and actual intercepts executed in Canada had decreased over the last couple of decades.<sup>5</sup> However, no Justice representative was able to explain why this decrease had occurred nor were any statistics forthcoming on the frequency with which intercepts were authorized, but abandoned for lack of technical ability to execute them: this crucial information is apparently not collected.

The lack of basic empirical data demonstrating the need for new law enforcement powers, particularly procedural amendments proposed under diluted judicial authorization, is disturbing. While many of the proposals in the consultation document may seem technical in nature and reasonable, it is not enough to abrogate constitutional protections by anecdote or for anything less than reasons which are demonstrably justifiable in a free and democratic society.<sup>6</sup> As the U.S. Supreme Court recognized one hundred and sixteen years ago, "[i]t may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing... by silent approaches and slight deviations from legal modes of procedure."<sup>7</sup>

---

<sup>2</sup> Canada, Dept. of Justice et al., *Lawful Access: Consultation Document* (Ottawa: Justice, 2002) [Lawful Access].

<sup>3</sup> Section 195 of the *Criminal Code* requires the Solicitor-General to annually publish reports on authorizations for interceptions of private communications (s. 185), authorizations given for emergency interceptions without reasonable diligence (s. 188), and interceptions made in the preceding year.

<sup>4</sup> M. Geist, "Federal proposal tells only part of cybercrime story" *The Globe & Mail* (3 Oct 2002); see also D. McCullagh, "Will Canada's ISPs become spies?" *News.com* (27 August 2002).

<sup>5</sup> See generally Canada, RCMP, *Annual Report on the Use of Electronic Surveillance As Required Under Section 195 of the Criminal Code* (Ottawa: RCMP, 1999) at 4, 11 (The Solicitor-General's annual report on the use of electronic surveillance indicates that the number of applications made for audio and video authorizations and renewals has fallen from 263 (1995) to 145 (1999). Total intercepts in 1999 was 879.

<sup>6</sup> *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11, s. 1 [Charter].

<sup>7</sup> *United States v. Bach*, (18 November 2002), No. 02-1238 (8<sup>th</sup> Cir. 2002) (Brief of *Amicus Curiae* Electronic Privacy Information Centre at 4) (citing *Boyd v. United States*, 116 U.S. 633 at 636 (1886)).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

*Does empirical data outside the consultation inform the public debate?*

In June 2002, the Institute for Security Technology Studies at Dartmouth College released a needs assessment on the technological impediments facing cybercrime investigators.<sup>8</sup> To assemble the data and prepare its findings, the ISTS conducted a national survey, held a workshop with key stakeholders in the law enforcement community, and interviewed law enforcement personnel, including investigators and prosecutors, in seven states and the District of Columbia.<sup>9</sup>

While the purpose of the assessment was to identify technological impediments and not necessarily legislative or regulatory impediments, it is difficult to divorce the two in cyberspace. "The *code* of cyberspace – its architecture and the software and hardware that implement that architecture – regulates life in cyberspace generally. Its code is its law."<sup>10</sup> Ironically, the report seemed to treat the technological imperative as surrogate for legislative and regulatory response:

"Laws, regulations, treaties, and other policy instruments have not evolved to match the new realities facing cyber-attack investigators.... [t]herefore, the struggle to stay technologically up-to-date promises to become a permanent feature of the law enforcement landscape."<sup>11</sup>

Conversely, many proponents of anti-cybercrime initiatives suggest that technological problems can and should be addressed by Draconian legal sanctions, even for *de minimis* infractions.<sup>12</sup>

The assessment identified a number of non-technical (or more correctly hybrid) issues commonly impeding cybercrime investigations, namely: insufficient record keeping by ISPs;<sup>13</sup> inability to effect data preservation extraterritorially;<sup>14</sup> encryption circumvention techniques;<sup>15</sup> and a lack of common data-sharing protocols.<sup>16</sup>

<sup>8</sup> M. Vatis, "The Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment" (Hanover, NH: Institute for Security Technology Studies, 2002), online: Dartmouth College <<http://www.ists.dartmouth.edu/lep/lena.htm>> (date accessed: 24 October 2002) [Needs Assessment].

<sup>9</sup> *Ibid.* at 10-12.

<sup>10</sup> L. Lessig, *The Future of Ideas: the fate of the commons in a connected world* (New York: Random House, 2001) at 35 [Lessig].

<sup>11</sup> Needs Assessment, *supra* note 8 at 10.

s.19(1)

<sup>12</sup> See e.g. [redacted] "Digital Copyright Reform in Canada: Reflections on WIPO and the DMCA" [unpublished] archived at *Lex Informatica*, online: <<http://www.lexinformatica.org/dox/digitalcopyright.pdf>> (date accessed: 12 November 2002) [Digital Copyright Reform]; see also *WIPO Copyright Treaty*, *infra* note 32, preamble ("recognizing the need to introduce new international rules and clarify the interpretation of certain existing rules in order to provide adequate solutions to the questions raised by... technological developments...").

<sup>13</sup> Needs Assessment, *supra* note 8 at 28-30.

<sup>14</sup> *Ibid.* at 30.

<sup>15</sup> *Ibid.* at 34 (The assessment did not make the distinction, but I enumerate this as a non-technical issue for the simple reason that brute force attacks on encrypted data are beyond the capacity of common computing. Any routine circumvention of encryption by law enforcement would employ largely non-technical methods, i.e. warrants for remote key-logging, assistance orders to compel production of passwords, etc.).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

The impediments identified were uniformly basic in nature (*i.e.* requirements for data collection tools that can parse information from multiple formats, automated and expert data collection tools to minimize requirements for investigator training, databases of subject experts in various jurisdictions, clearinghouses for tools and techniques, investigative tools specifically designed for law enforcement, etc.), suggesting that many of the difficulties investigators now face would be more appropriately addressed in Silicon Valley than in Parliament, Congress or Brussels.<sup>17</sup>

**What are Canada's legal obligations under the Council of Europe's *Convention on Cyber-crime*?**

In February of 1997, the Council of Europe created a Committee of Experts on Crime in Cyberspace to draft "a binding legal instrument" dealing with the creation of new computer-related offences, substantive criminal law, the use of national and international coercive powers and jurisdiction.<sup>18</sup>

The first public draft was not released until April, 2000 and was criticized by civil society groups as being incomplete in that it lacked the most controversial procedural amendment: lawful access to real-time communications data.<sup>19</sup> The final text was released in June 2001 and opened for signature in September 2001.

On November 23, 2001, Canada, along with 30 other nations, signed the Council of Europe's *Convention on Cyber-crime*.<sup>20</sup> The stated purpose of the *Convention* is threefold: to harmonize the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime; to provide for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences

---

<sup>16</sup> *Ibid.* at 24 (this complaint is ironic given that the greatest threat to network neutrality is the desire by law enforcement and commercial actors to build intelligence into the network. Here, the law enforcement community recognizes the value neutral protocols have had for the development of the Internet, seemingly wish to emulate that success for investigatory data-sharing, but also seek to optimize the network for one set of uses, namely: authentication, integrity and non-repudiation.); see e.g. J. Speta, "A Common Carrier Approach to Internet Interconnection" (2002) F54 F.C.L.J. 274-275:

"[B]uilding complex functionality into a network implicitly optimizes the network for one set of uses while substantially increasing the cost of a set of potentially valuable uses that may be unknown or unpredictable at design time. The number of new applications developed for the Internet – from browsing, to Napster, to instant messaging – is a testament to that system's flexibility." [footnotes omitted]

<sup>17</sup> *Ibid.* at 52 ("The entities that develop technological solutions to the obstacles outlined in this study have a singular opportunity. Since the existing technology does not meet cyber-attack investigators' needs, the solutions that are developed may become widely adopted by the law enforcement community.").

<sup>18</sup> See Council of Europe, 646a(2001) News Release "First international treaty to combat crime in cyberspace approved by Ministers' Deputies" (19 September 2001); Explanatory Report, *infra* note 22 at paras. 7-15.

<sup>19</sup> The first public draft was number 19; the real-time collection of traffic data provision did not reappear until draft 27.

<sup>20</sup> Council of Europe, Committee of Ministers, 109<sup>th</sup>, *Convention on Cyber-crime*, ETS No. 185. (2001) [Convention].



*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

as well as other offences committed by means of a computer system; and, to create an efficient and effective regime of international cooperation.

*The structure of the Convention*

The *Convention* contains four chapters: I) definitions; II) measures to be taken at domestic level – substantive law and procedural law; III) international co-operation; IV) and final clauses.

These comments briefly review the substantive law offences (Section 1, Chapter II), in an attempt to identify amendments necessary for Canadian ratification of the *Convention*. The second part and primary focus of this discussion addresses some of the implications of proposed procedural law amendments (Section 2, Chapter II), by reference to current Canadian law and other norms, including a discussion on the nature of "traffic data".

Substantive Law Obligations

Canadian law already recognizes the offences found in Articles 2 through 5, dealing with illegal access, illegal interception, data interference and system interference.<sup>21</sup>

Article 6 establishes a separate and independent criminal offence from Articles 2 through 5. To attract sanction, an individual must produce, sell, procure for use, import, distribute or otherwise make available a device or data (e.g. a computer password) capable of accessing a computer system *and* possess *and* use the prohibited thing with the intention of committing one of the illegal acts specified in Articles 2 through 5.

According to the Explanatory Report to the *Convention on Cyber-crime*, the general intent clause is restricted to devices that are "objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices."<sup>22</sup> The *Lawful Access* document does not offer an alternate standard, but simply notes that "offences in relation to illegal devices (such as viruses) would have to be added. These could include importation, procurement for use, and otherwise making available an illegal device as defined in the *Convention*."<sup>23</sup>

The doctrine of contributory liability is grounded in the recognition that effective attribution of fault may require the courts to look beyond the primary act to the means that make the offence possible. In so doing, the law must strike a balance between legitimate efforts to target criminal behaviour and the rights of others to engage in substantially unrelated areas of commerce and free expression.<sup>24</sup> Accordingly, the

<sup>21</sup> R.S.C. 1985, c. C-46, s. 183-184, 342.1, 342.2, 430 [*Criminal Code*]; *R. v. Weir* (1998), [1998] A.J. No. 155 at para. 77 (C.A.), *aff'd* [2001] A.J. No. 869.

<sup>22</sup> Explanatory Report to the *Convention on Cyber-crime*, *infra* note 20 at para. 73 [Explanatory Report].

<sup>23</sup> *Lawful Access*, *supra* note 2 at 14.

<sup>24</sup> To do otherwise would contravene s. 2(b) of the *Charter*.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

production, sale, procurement for use, import, distribution or otherwise making available of devices or data capable of prohibited access should not attract criminal liability if the device or data could be used for commercially significant non-infringing uses,<sup>25</sup> even if the purpose for any of the above, under an objective standard, might otherwise be prohibited. This is a narrower and more utilitarian-based approach than that proposed in the *Convention* and implicitly adopted in the *Lawful Access* document, yet it is consistent with approach taken by the courts in other contexts.

Articles 7 and 8 deal with computer-related fraud and forgery. Canadian law already recognizes the offences of fraud<sup>26</sup> and forgery<sup>27</sup> in a media-neutral fashion, such that any amendments would be largely technical.

Article 9 adopts minimum requirements for the establishment of criminal offences relating to child pornography.<sup>28</sup> The recent Supreme Court decision in *R. v. Sharpe*,<sup>29</sup> found that the prohibition of the possession of child pornography exclusively for personal use was regulation of expression bordering on thought and an unjustifiable infringement of s. 2(b) of the *Charter*.<sup>30</sup> This suggests that Canada may need to reserve s. 9(1)(e) of this part.<sup>31</sup>

Article 10 deals with offences related to the infringement of copyrights and related rights and requires parties to adopt criminal sanctions for willful copyright infringement on a commercial scale and by means of a computer system.

The *Convention* defers substantive treatment of copyright offences to *inter alia* the WIPO Internet Treaties.<sup>32</sup> It is beyond the scope of these comments to engage in a detailed or

<sup>25</sup> See e.g. *Sony Corp. v. Universal City Studios, Inc.*, (1984) 464 U.S. 417 at 442 (no contributory liability if capable of commercially significant non-infringing uses); see also M. B. Nimmer, *Nimmer on Copyright*, vol. 3, looseleaf (Albany, NY: Matthew Bender, 1978) c. 12A at §12A.19, arguing that § 1201(a)(2) of the *Digital Millennium Copyright Act* largely ventilates the general application of *Sony* by proscribing devices or services that fall within any one of the following three categories: they are primarily designed or produced to circumvent; they have only limited commercially significant purpose or use other than to circumvent; or they are marketed for use in circumventing.

<sup>26</sup> *Criminal Code*, *supra* note 21 at s.366, 368, 372(1), 374, 375, 376(2) (an exception may be s. 371 which is triggered only by a "telegram, cablegram or radio message...").

<sup>27</sup> *Ibid.* at s. 380, 382-384, 387-389, 400; see e.g. *American Technology Exploration Corp. (Re)* (January 23, 1998), COR #98/013 (B.C. Sec. Comm.) (finding that respondent "ATEC used the modern technology of the Internet for an old fashioned purpose promoting its shares with outrageous misrepresentations" and providing sanctions).

<sup>28</sup> *Ibid.* at s. 163(1), 163.1

<sup>29</sup> [2001] 1 S.C.R. 45.

<sup>30</sup> *Ibid.* at paras. 108 and 129.

<sup>31</sup> The federal government recently introduced Bill C-20, *An Act to amend the Criminal Code (protection of children and other vulnerable persons) and the Canada Evidence Act*, 2d Sess., 37<sup>th</sup> Parl., 2002, cl. 7 (1<sup>st</sup> reading 5 December 2002) which would tailor the definition of "child pornography" in s. 163.1 capture "any written material the dominant characteristic of which is the description, for a sexual purpose, of sexual activity with a person under the age of eighteen years that would be an offence under this Act, regardless of motive."

<sup>32</sup> See *WIPO Copyright Treaty*, Dec. 20, 1996, 36 I.L.M. 65, WIPO Publ. No. 226(E); *WIPO Performances and Phonograms Treaty*, Dec. 20, 1996, 36 I.L.M. 76, WIPO Publ. No. 227(E) [Internet Treaties].

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

technical discussion of digital copyright reform, not least because Industry Canada and the Department of Canadian Heritage have already concluded their public consultation on the ratification of the Internet Treaties.<sup>33</sup> However, to the extent that the *Convention* seeks to reinforce the necessity of criminal sanctions for copyright infringement, these comments raise two points.

The Explanatory Report observes, with regard to this article:

"The ease with which unauthorized copies may be made due to digital technology and the scale of reproduction and dissemination in the context of electronic networks *made it necessary* to include... *criminal law sanctions* and enhance international co-operation in this field." [Emphasis added]<sup>34</sup>

First, the argument that current copyright laws are not strong enough and that more stringent, criminal provisions need be adopted is discredited by the fact that, in the U.S., private personal copying has only increased in the aftermath of the adoption of harsher criminal sanctions since the late 1990's.<sup>35</sup> Adopting new criminal sanctions for *de minimis* or intermediary infringement can only serve to uncouple remedies from alleged harms, as many charge has already occurred in the U.S.<sup>36</sup>

It may be entirely appropriate to argue that criminal sanctions are the only effective response to 'piratical' conspiracies for commercial copyright infringement. Aside from 'aiding and abetting' in Article 11, this is the only criminal copyright offence called for in the *Convention*,<sup>37</sup> but those who are concerned with sophisticated commercial bootlegging schemes should advocate for a specific conspiracy offence and not a general offence that applies to inconsequential copyists.<sup>38</sup>

The Internet Treaties stop short of actually calling for criminal sanctions<sup>39</sup> and the *Convention* allows reservations for the imposition of criminality *as long as other effective*

---

<sup>33</sup> See Canada, Industry Canada, *Supporting Culture And Innovation: Report on the Provisions and Operation of the Copyright Act* (Ottawa: Intellectual Property Policy Directorate, 2002) [Section 92 Report].

<sup>34</sup> Explanatory Report, *supra* note 22 at para. 107.

<sup>35</sup> S Biegel, *Beyond Our Control*, (Cambridge: MIT Press, 2001) at 297.

<sup>36</sup> M. Godwin, "Technology vs. Technology: Should Code-breakers Go To Jail? The Limits of Anti-circumvention" (5<sup>th</sup> Annual Technology & Society Conference, Cato Institute, 14 November 2001) [unpublished], online: Cato Institute <<http://www.cato.org/events/futureip/panel3-godwin.pdf>> (date accessed: 4 December 2001) at 8.

<sup>37</sup> *Convention*, *supra* note 20 at Art. 10(1),(2) ("Each Party shall adopt... measures as may be necessary to establish as criminal offences [for] the infringement of copyright,... where such acts are committed willfully, on a commercial scale....").

<sup>38</sup> A. A. Keyes and C. Brunet, *Copyright in Canada: Proposals for Revision of the Law* (Ottawa: Consumer and Corporate Affairs Canada, 1977) at 185 cited in Young, *supra* note 42, n. 45; *Criminal Code*, *supra* note 21 at s. 467.1(1) (indictable offence for knowingly participating in a criminal organization).

<sup>39</sup> Internet Treaties, *supra* note 32 at WCT Art. 18 and WPPT Art. 19, respectively (It seems clear that criminal sanctions are suggested in that the language differentiates between *legal remedies* for someone who knowingly tampers with rights management information and *civil legal remedies* for someone who reasonably should know.).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

remedies, including civil and/or administrative measures, are available.<sup>40</sup> Therefore, Canada is not obligated to create new criminal copyright offences under either treaty.<sup>41</sup> The Law Reform Commission of Canada has cautioned that criminal sanctions in copyright are blunt instruments and should be employed with great caution.<sup>42</sup> Not only is criminality ineffective in dissuading the behaviour government purports to target, these kinds of sanctions would not be proportionate responses, as required under Article 13 of the *Convention*.<sup>43</sup>

The second point with regards to Article 10 concerns privacy. Copyright law has traditionally been compatible with privacy because it was confined to the administration of *public distribution* of copyright works. However, digital rights management ("DRM") systems expand the scope of – some would say introduce new – exclusive rights to control *private consumption*.

"Today, individuals are free to explore different ideas presented in books, music, and movies anonymously. Existing DRM systems weaken this right by allowing copyright owners to monitor private consumption of content. In an attempt to secure content, many DRM systems require the user to identify and authenticate a right of access to the protected media."<sup>44</sup>

The government should recognize and seek to minimize the extent to which the infringement of privacy rights, in the name of copyright protection, implicates the state on behalf of private actors (*i.e.* criminalization of: anti-circumvention of copyright protection even for 'fair dealing' purposes; *de minimis* infringement), particularly foreign actors who may operate under more stringent copyright regimes.

Article 11 requires parties to apply criminal sanctions for intentionally aiding and abetting the commission of offences in Articles 2 through 10. In some cases Canadian law already recognizes liability for third-party involvement in the commission of these offences (*i.e.* permitting unauthorized use of a password by a third-party),<sup>45</sup> but not in

<sup>40</sup> Explanatory Report, *supra* note 22 at para. 116.

<sup>41</sup> The question tabled before the s. 92 parliamentary committee reviewing the *Copyright Act* asks "whether section 42 of the *Act* should be amended to set a minimum value of the infringing copies in order to be subject to criminal remedies" and suggests that this would be appropriate. However, it also implies a minimum value of \$1000 by reference to the U.S. floor of the same amount, Section 92 Report, *supra* note 33 at 26-27. In the age of peer-to-peer file-sharing, this would capture most Canadian teenagers. Additionally, a simple number does little to reflect the economic benefit copyright holders may derive from increased public exposure of their works.

<sup>42</sup> A. Young, "Catching Copyright Criminals: *R. v. Miles of Music Ltd.* (1990) I.P.J. 257 (citing a 1976 Law Reform Commission of Canada recommendation).

<sup>43</sup> *Convention*, *supra* note 20 at Art. 13 (requiring "effective, proportionate and dissuasive sanctions").

<sup>44</sup> C. Hoofnagle, J. Young and N. Anastasopoulos, "Digital Entertainment and Rights Management" Comments before the Technology Administration, U.S. Department of Commerce (July 17, 2002), online: EPIC <<http://www.epic.org/privacy/drm/tadrmcomments7.17.02.html>> (date accessed: 5 Nov 2002); see generally Ontario, IPC, *Privacy and Digital Rights Management (DRM): An Oxymoron?*, (Toronto: IPC, 2002), online: IPC <<http://www.ipc.on.ca/english/pubpres/papers/drm.pdf>> (date accessed: 5 Nov 2002).

<sup>45</sup> *Criminal Code*, *supra* note 21, s. 342.1(1)(d).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

other instances (*i.e.* normal activities of an ISP do not implicitly authorize content providers to communicate the material that they have posted on the server).<sup>46</sup> The issue of potential liability under the *Copyright Act*<sup>47</sup> will be particularly influential in shaping future participation on the Internet.<sup>48</sup>

According to the Explanatory Report:

"Liability [under this section] arises... where the person who commits a crime... is aided by another person *who also intends that the crime be committed*. For example, although the transmission of harmful content data or malicious code through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section. Thus, there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision."<sup>49</sup>

This statement is in general accordance with current Canadian jurisprudence,<sup>50</sup> although intent can also be implied in circumstances in which an intermediary has sufficient knowledge of infringing activity.<sup>51</sup>

Article 12 requires parties to adopt measures to ensure that legal persons (corporations) can be held liable for a criminal offence committed for their benefit by a director, or under the authority of a director, of the corporation. In most scenarios this would be an uncontentious issue, however in the copyright context, a plain reading of this section could be interpreted as attributing criminal, administrative or civil liability to telecommunications or Internet service providers for aiding or abetting copyright infringement by its failure to monitor the conduct of its subscribers.

### Procedural Obligations

Section 2 of Chapter II of the *Convention* establishes broad procedural powers for the purpose of criminal investigation of the offences established in Section 1, Articles 2 through 11. However, the procedural powers are not limited to only these offences or

<sup>46</sup> *SOCAN v. CAIP et al.*, [2002] FCA 166 at para. 161, leave to appeal to S.C.C. requested.

<sup>47</sup> R.S.C. 1985, c. C-42 [Tariff 22 Appeal].

<sup>48</sup> Tariff 22 Appeal, *supra* note 46. (Affidavit of Professor Michael Geist in support of motion for leave to appeal) at para. 9 (on file with author).

<sup>49</sup> Explanatory Report, *supra* note 22 at para. 119.

<sup>50</sup> See *Vigneux v. Canadian Performing Right Society Ltd.* (1945), 4 C.P.R. 65 (no authorizing infringement absent right to authorize); *Muzak Corp. v. Composers, Authors & Publishers Assn. (Canada)*, [1953] 2 S.C.R. 182 (authorization presumed granted only in accordance with the law); *de Tervagne v. Beloil* (1993), 50 C.P.R. (3d) 419 (T.D.) (authorization must sanction, approve or countenance more than mere use of equipment that might possibly be used in an infringing performance but, need not go so far as to grant or purport to grant the right to perform).

<sup>51</sup> *CCH Canadian v. Law Society of Upper Canada*, 2002 FCA 187 (authorization implied where means to infringe provided and controlled by authorizer, who is aware of sufficient evidence of infringement, but takes no steps to discourage it).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

even to 'cybercrimes' generally.<sup>52</sup> The *Convention* is directed at any criminal offence committed by means of a computer system and the collection of evidence of any criminal offence, where that evidence is in electronic form.<sup>53</sup>

There are two exceptions to this scope of application. First, Article 21 provides that the power to intercept content data shall be limited to a range of serious offences to be determined by domestic law. Second, a party may reserve the right to apply the measures in Article 20 (real-time collection of traffic data) only to specific offences or categories of offences.<sup>54</sup>

The Explanatory Report cautions against adopting the Article 20 reservation, based on the importance of real-time tracing communications and on the grounds that "the collection of traffic data alone does not collect or disclose the content of the communication" and is therefore less subject to a lower expectation of privacy.<sup>55</sup>

The Dartmouth needs assessment identified real-time traffic data collection as one of the most effective methods of catching cyber criminals.<sup>56</sup> According to the *Lawful Access* document, real-time search of traffic data is already permissible in Canada under either s. 487.01 or Part VI of the *Criminal Code*, but suggests that the standard for Internet traffic data should be more in line with that required for telephone records and dial number recorders:

"[I]n light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication... [a] specific production order could be created under a lower standard in order to allow for the production of telecommunications associated data, that extends beyond the telephone numbers already covered by section 492.2 of the *Criminal Code*, historic traffic data or real-time collection of traffic data."<sup>57</sup>

Again, the *Lawful Access* document does not provide any background as to why a lower judicial standard is required, but from other sources we learn that the argument is premised on a number of inter-related themes: traffic data is of great evidentiary value to law enforcement and rapid collection is crucial to ensuring availability and integrity of

<sup>52</sup> See generally S. Brenner, "Is There Such a Thing as 'Virtual Crime'?", (2001) 4 *Cal. Crim. Law Rev.* 1 (author concludes that most of the activity currently characterized as "cybercrime" is nothing more than the commission of conventional crimes by unconventional means).

<sup>53</sup> *Convention*, *supra* note 20, Art. 14(2)(a-c).

<sup>54</sup> Explanatory Report, *supra* note 22 at paras. 142-43 (the article 20 reservation is subject to the exception that the reservation cannot be narrower than the powers reserved under article 21).

<sup>55</sup> *Ibid.*

<sup>56</sup> Needs Assessment, *supra* note 8 at 30.

<sup>57</sup> *Lawful Access*, *supra* note 2 at 11-12; see also Canada, CRTC, Provision of subscribers' telecommunications service provider identification information to law enforcement agencies, Telecom Order 2001-279, (Ottawa: CRTC, 2001) at para. 11 (finding that LSPID information does not reveal intimate details of the lifestyle or personal choices of subscribers, but can only be provided to law enforcement under certain conditions); Canada, CRTC, *Bell Canada – Customer Name and Address*, Telecom Decision 2002-52, (Ottawa: CRTC, 2002) at para. 17 (information in a reverse-directory is non-confidential; value of warrantless access outweighs the privacy concerns in providing the information).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

the data; it is often difficult to collect this data; and many parties argue that it attracts a lower expectation of privacy than content data.

No stakeholder in this debate questions the evidentiary value of traffic data; clearly, it is an important piece of the cybercrime puzzle. However, when it comes to addressing the best method of getting this evidence into the hands of law enforcement while maintaining adequate protections for privacy, the consensus breaks down.

The Department suggests that the problem is a lack of lawful access to the requisite data, but provides no reasoning for this implied conclusion. Meanwhile, the Dartmouth needs assessment identified the primary impediments to real-time collection of traffic data as technological (*i.e.* software not specifically designed for law enforcement) and administrative (*i.e.* lack of coordination between jurisdictions, particularly internationally).

The *Lawful Access* document suggests production orders for income tax information and tracking devices for dial number recorders are analogous precedents for diluted judicial authorization for search and seizure of traffic data. But it is not difficult to distinguish these categories of information from most traffic data protocols: the former is collected for a necessary regulatory purpose, while the latter reveals much less "about one's lifestyle, intimate relations or political or religious opinions"<sup>58</sup> than many forms of network traffic data.<sup>59</sup>

The *Lawful Access* document addresses the adoption of a general production order; a specific production order for traffic data; and, a specific production order for subscriber and/or service provider information. Since the criticisms of the proposed procedural amendments apply regardless of the order power sought, it would be appropriate to depart from an article-by-article analysis of the *Convention* and instead turn to an issues-based approach.

**Diluted judicial oversight of electronic surveillance is unconstitutional.**

*The rationale for judicial pre-authorization for electronic surveillance.*

The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private.<sup>60</sup> A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we send an email or visit a web site might be superbly equipped to fight crime, but would be one in which privacy no longer

<sup>58</sup> Millar, *infra* note 87 and accompanying text.

<sup>59</sup> See Appendix A for examples of traffic data in different network applications.

<sup>60</sup> *R. v. Duarte*, [1990] 1 S.C.R. 30 at para. 24 [*Duarte*].



*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

had any meaning. It is unacceptable in a free society that the agencies of the state be free to use this technology at their sole discretion.<sup>61</sup>

In one of the first cases decided under the *Charter of Rights and Freedoms*, the Supreme Court wrote:

"The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement."<sup>62</sup>

Consequently, the *Criminal Code* generally prohibits law enforcement from obtaining documents or information without first establishing a factual foundation of 'reasonable and probable' grounds that an offence has been or will be committed. This requirement serves two purposes: first, it is a check against the "unfettered discretion"<sup>63</sup> of law enforcement to look for and collect evidence of crime at the expense of individuals' *Charter* rights; and, second, it creates a record of accountability subject to audit of abuse of authority and defects in the law.

In *R. v. Duarte*, La Forest J. recognized Parliament's efforts, in Part IV.1 of the *Criminal Code*, to strike a reasonable balance between the right of individuals to be left alone and the right of the state to intrude on privacy in the furtherance of detecting and prosecuting criminal activity:

"Law enforcement must always seek *prior judicial authorization* before using electronic surveillance. Only a superior court judge can authorize electronic surveillance, and the legislative scheme sets a high standard for obtaining these authorizations. A judge must be satisfied that other investigative methods would fail or have little likelihood of success, and that the granting of the authorization is in the best interest of the administration of justice... this latter prerequisite imports as a *minimum requirement* that the issuing judge must be satisfied that there are reasonable and probable grounds to believe that an offence has been or is being committed and that the authorization sought will afford evidence of that offence. [T]he provisions and safeguards of the *Code* have been designed to prevent the agencies of the state from intercepting private communications on the basis of mere suspicion." [Emphasis added]<sup>64</sup>

---

<sup>61</sup> *Ibid.* at paras. 24ff.

<sup>62</sup> *Hunter v. Southam*, [1984] 2 S.C.R. 145 at 166-67.

<sup>63</sup> *Duarte*, *supra* note 60 at paras. 23.

<sup>64</sup> *Ibid.* at para. 26.



*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

*Production orders are as legally invasive as warrants because s. 8 protects people, not places or things.*

The Department of Justice proposes the creation of a specific production order which would grant law enforcement access to "traffic data" under a lower judicial standard than required for a warrant or intercept. The Supreme Court has ruled that an order for the production of documents is a seizure within the meaning of s. 8 of the *Charter of Rights and Freedoms*,<sup>65</sup> as is the power to make copies of documents.<sup>66</sup> Therefore, an order for the production of records made pursuant to the *Code* would fall under the ambit of s. 8 of the *Charter*.

The Department suggests that a lower standard for production orders is justified because these orders would be "less intrusive than a search warrant as there would be no entry into and search by law enforcement of the premises of a third-party." This overemphasizes the purely physical aspect of a search and seizure at the expense of the impact on the individual to whom the search was targeted and the seized information pertained. In *R. v. Edwards*,<sup>67</sup> the Supreme Court held that "an interpretation of the degree of intrusiveness is not a matter of where the information in question is located, but to what extent disclosure of that information would impact the reasonable expectation of the individual's privacy." It is a well-established principle that s. 8 protects "people, not places or things".<sup>68</sup>

With some irony, these comments note the apologetic reminder of the Court in *R. v. O'Connor*:

"Although it may appear trite to say so, I underline that when a private document or record is revealed and the reasonable expectation of privacy therein is thereby displaced, the invasion is not with respect to the particular document or record in question. Rather, it is an invasion of the dignity and self-worth of the individual, who enjoys the right to privacy as an essential aspect of his or her liberty in a free and democratic society."<sup>69</sup>

In consideration of a search and seizure of an ISP subscriber's email, the U.S. 8<sup>th</sup> Circuit in *United States v. Bach*<sup>70</sup> recently found that a lawful search by a third party can be reasonable, implying that it is not always so, though it declined to find on the facts.<sup>71</sup>

<sup>65</sup> See e.g. *Thomson Newspapers*, *infra* note 105; *R. v. McKinlay Transport Ltd.*, [1990] 1 S.C.R. 627.

<sup>66</sup> See e.g. *Comité paritaire de l'industrie de la chemise v. Potash*, [1994] 2 S.C.R. 406.

<sup>67</sup> [1996] 1 S.C.R. 128 at para. 34.

<sup>68</sup> See *R. v. Colarusso*, [1994] 1 S.C.R. 20 at 60 (*per* La Forest J.); see also *R. v. Plant*, [1993] 3 S.C.R. 281 at 291; *Hunter*, *supra* note 62 at 158, citing *Katz v. United States*, 389 U.S. 347 (1967); and *R. v. Dymnt*, [1988] 2 S.C.R. 417 at 428-29.

<sup>69</sup> [1995] 4 S.C.R. 411 at para. 131.

<sup>70</sup> *United States v. Bach*, (18 November 2002), No. 02-1238 (8<sup>th</sup> Cir. 2002).

<sup>71</sup> *Ibid.* at 6 (the Court wrote that "[c]ivilian searches are sometimes more reasonable than searches by officers." and then reviewed a number of situations in which this might be true. According to both the Yahoo! *et al.* amicus brief and the government's *factum* in the appeal, when executing warrants, ISP technicians do not selectively choose or review the contents of the named account, they simply hand over

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

*Third-party intermediaries would not have standing under s. 24 of the Charter for infringements of subscribers' privacy*

The Department's assertion that a search of third-party holders of information would be "less invasive" also ignores the question of the availability of remedy intrinsic to any determination of invasiveness. The contours of a *Charter* remedy do much to govern the shape of the protected right. "The question of breach must, therefore, be assessed in terms of the interests protected by the section and such remedy as the court can provide to secure them."<sup>72</sup>

An individual would have no knowledge of a search of personal information held by a third-party and therefore no ability to challenge the reasonableness of a search. Current search and seizure and interception law requires notification of the subject of a search or interception after the fact,<sup>73</sup> it would seem at least a partial solution to require that any production order standard incorporate the same requirement.

In claiming that a third-party search would be "less invasive" the Government wrongly foists responsibility for seeking remedies for s. 8 breaches on third-parties with no standing under s. 24(1) to enforce them, even were they so inclined to do so (*i.e.* in the public interest). In *R. v. Thompson*,<sup>74</sup> Sopinka J. was careful to point out that the invasion of third-party privacy rights is not determinative of the reasonableness of the search. Moreover, a plain reading of s. 24(1) does not support an interpretation of automatic standing, which reads as follows:

*Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.*  
[Emphasis added]

Wilson J. in *Rahey* interpreted s. 24(1) as providing application for remedy only to a person whose rights under the *Charter* have been infringed.<sup>75</sup> This would necessarily exclude third party standing, even were telecommunications and Internet service providers so inclined to act as guardians of their subscribers' privacy rights.

Section 24(1) is not an exclusive remedy for breach of the *Charter*.<sup>76</sup> Nor is it necessary for an applicant to argue anything more than a breach of his or her s. 8 rights to invoke a remedy under s. 24(1) or s. 52(1). Any court seized of the dispute has the power and the

---

the entire contents in response to a subpoena. This can hardly be seen as less intrusive, given that if the search had been conducted properly by law enforcement, they would be restricted to the terms of the warrant [Emphasis added]).

<sup>72</sup> *R. v. Rahey*, [1987] 1 S.C.R. 588 at para. 111.

<sup>73</sup> *Criminal Code*, *supra* note 21 at s. 189 (5) (notice of intention to produce evidence), s. 196 (notification required after interception), s. 487.01(5.1) (notice required after covert entry).

<sup>74</sup> [1990] 2 S.C.R. 1111 at 1143-1144.

<sup>75</sup> [1987] 1 S.C.R. 588 at para. 61.

<sup>76</sup> *R. v. Big M Drug Mart*, [1985] 1 S.C.R. 295 at para. 37.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

duty to determine the validity of the statute.<sup>77</sup> However, it seems clear that a s. 52(1) remedy is narrower than the range granted under s. 24(1). The severance of the s. 24(1) remedy or range of remedies for lack of standing seems significant, particularly in the context of proposed routinized surveillance of subscribers by intermediaries acting as 'agents of the state'.<sup>78</sup> This is an admittedly inchoate argument, but one which should not be ignored.<sup>79</sup>

Telecommunications and Internet service providers will be one of the first impartial checks against unreasonable search and seizures, particularly under any scheme of diluted judicial oversight. Presented with narrowed constitutional redress, intermediaries will be less inclined to resist unreasonable investigatory demands by law enforcement, even in circumstance when they feel that they are unreasonable.

*Information produced for criminal investigations attracts greater judicial scrutiny than information collected for other purposes.*

The Department of Justice suggests that because "production orders already exist in some federal laws, such as the *Competition Act*" a precedent has been set to create new order in the *Criminal Code*. This comparison fails to distinguish the inquisitorial and compulsive nature of criminal investigations from the regulatory investigations of the *Competition Act* and other statutes.

In *R. v. Fitzpatrick* the Court applied the lower expectation standard to records "that are statutorily compelled as a condition of participation in the regulatory area. Little expectation of privacy can attach to these documents, since they are produced precisely to be read and relied upon by state officials."<sup>80</sup> However, the Court distinguished these records and records in the criminal context: "searches and seizures of documents relating to activity known to be regulated by the state are not subject to the same high standard as searches and seizures in the criminal context." [Emphasis added]

The Court observed that "the requirement to keep records under the *Fisheries Act* does not impose any psychological or emotional pressures on the individual, and in this way the state intrusion at issue here contrasts sharply with inquisitorial and police interrogatories and testimonial compulsion."<sup>81</sup> [Emphasis added]

Similarly, in *British Columbia Securities Commission v. Branch*,<sup>82</sup> Sopinka and Iacobucci JJ., in finding that business and personal records deserved different protection,

<sup>77</sup> P. Hogg, *Constitutional Law of Canada*, 4<sup>th</sup> ed. (Toronto: Carswell, 1999) at 791.

<sup>78</sup> *Ibid.* at 773.

<sup>79</sup> See e.g. *Rahey*, *supra* note 72 (comparing the interpretations of Wilson and La Forest JJ. on the theory that the contours of a remedy give shape to the right.)

<sup>80</sup> [1995] 4 S.C.R. 154 at para. 49.

<sup>81</sup> *Ibid.* para. 51.

<sup>82</sup> [1995] 2 S.C.R. 3.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

favourably considered the analysis of the judge at trial in finding that the purpose of the *Securities Act* was "regulatory and administrative, not criminal or quasi-criminal".<sup>83</sup>

**'Traffic data' should attract a reasonable expectation of privacy.**

*The Department of Justice fails to distinguish the nature of traffic data.*

The Department of Justice next attempts to justify a lower judicial pre-authorization for production orders on the assumption that individuals have a lower expectation of privacy in traffic data than they would in other categories of data.

However, the Explanatory Report makes a valuable distinction which the *Lawful Access* document does not.

"[T]he privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind...."<sup>84</sup>

*A contextual analysis of the nature of traffic data suggests it would often attract a higher expectation of privacy than the Lawful Access document claims.*

In *R. v. Mills* the Supreme Court wrote: "the interest in being left alone by the state includes the ability to control the dissemination of confidential information."<sup>85</sup> As La Forest J. stated in *Duarte*: "...it has long been recognized that this freedom not to be compelled to share our confidences with others is the very hallmark of a free society."<sup>86</sup>

Over two hundred years ago, an English court found, in law, an symbiotic relationship between information privacy and identity. Yates J., in *Millar v. Taylor*:

"It is certain every man has a right to keep his own sentiments, if he pleases: he has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends." Privacy concerns are at their strongest where aspects of one's individual identity are at stake, such as in the context of

<sup>83</sup> *Ibid.* at para. 25; see Appendix A for an example of the kind of information that can be gleaned from a web site's HTTP-Referrer log or similar.

<sup>84</sup> Explanatory Report, *supra* note 22 at para. 227.

<sup>85</sup> [1999] 3 S.C.R. 668 at para. 80.

<sup>86</sup> [1995] 1 S.C.R. 30, at 53-54.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

information "about one's lifestyle, intimate relations or political or religious opinions"<sup>87</sup>

Sopinka J., writing for the Court in *R. v. Plant* found that "it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."

It would be incorrect to interpret Sopinka's 'biographical core' as an enumeration of categories of information in which individuals would have a reasonable expectation of privacy. Labels should not be determinative in deciding whether constitutional protection extends. Instead, one must look at the total context of the particular information in question.<sup>88</sup> There are categories of information which, perhaps by statutory definition, have been labeled "personal and confidential" in nature e.g. financial and health records. These categories of information, for public policy reasons, may always reside within the legal protection of the biographical core. However, in observing that "[a biographical core] would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual" the Court in *Plant* recognized that it is not the label which renders the information "personal" or "intimate", but the context. An individual's name in a phone book will attract a lower expectation of privacy than if it was found on a list of credit card debtors; meanwhile, that individual's name on an otherwise blank sheet of paper in an airport lounge will likely not attract any privacy interest.

Similarly, network traffic data in the hands of the average person may not be personally-identifiable, but could take on a very different significance in the possession of a telecommunications or Internet service provider or law enforcement with access to the contextual techniques with which to interpret it. Under these circumstances, otherwise non-personally-identifiable data could easily "reveal intimate details of an individual's personal lifestyle or private decisions".

The nature of the content of the information is not the only determinant for extending constitutional protection. For example, in *R. v. Shearing* the Court's analysis of the nature of the information contained in a diary was secondary to whether the owner of the diary had a reasonable expectation of privacy in the contents:

"It was a diary. Diaries are supposed to be private. [T]he fact that [the owner] specifically chose to record her thoughts and recollection of daily events in a private, locked diary, rather than, for instance, on a calendar on her bulletin board, post-it notes on the refrigerator, or even her school notebook, suggests to me that she had a high expectation of privacy in what she wrote, *regardless of its content*. Counsel for the complainant persuasively observed at trial that 'the issue surely with respect to privacy is the respect these courts are prepared to pay to the individual's ability to write down whatever he or she may choose to write down in

<sup>87</sup> (1769), 4 Burr. 2303, 98 E.R. 201 at 2379 and 242 [Millar].

<sup>88</sup> *R. v. Wholesale Travel Group Inc.*, [1991] 3 S.C.R. 154 at 209 ("what is ultimately important are not labels (though these are undoubtedly useful), but the values at stake in the particular context").

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

one's personal diary. That's the privacy interest at stake, it's not what is written down.' She went on to draw a powerful analogy between the diary and private therapy records: "So for example, what if in therapy one didn't talk so much about one's feelings but about one's taste in shopping? It would not, in my submission, detract from the reasonable expectation of privacy to be able to establish that the content of the conversation was X rather than Y."<sup>89</sup> [Emphasis added]

Similarly, in *R. v. Law*,<sup>90</sup> the Supreme Court did not examine the contents of the private documents to evaluate the owner's privacy interest. In that case, thieves stole a safe containing commercial documents from two restaurant owners. The police recovered the safe, but before it was returned to the owners, an officer who suspected the owners of tax violations photocopied some of the documents inside and eventually forwarded the photocopies to Revenue Canada. Bastarache J., writing for the Court, concluded that the owners' reasonable expectation of privacy in their documents derived not from their contents, but from the fact that they chose to keep the documents confidential by locking them in a safe. In its reasoning, the Court noted that informational privacy "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain ... as he sees fit."<sup>91</sup>

A reasonable expectation of privacy is not premised on the location of the information in which the expectation is held, as the Federal Court of Appeal held in *Del Zotto v. Canada (Minister of National Revenue)*.<sup>92</sup> The Court found that the appellant had a reasonable expectation of privacy over documents and information held by other people at different places because they "could reveal incredibly intimate and personal details about his preferences, habits, opinions, hopes and activities." Characterizing it as "a window into most of a person's private life" the documents contemplated by the Court included reading materials, relationships with churches, charities or political parties, personal tastes, relationships with other people and documents relating to the appellant's financial affairs. Information of this nature could clearly be the target of any production order for a telecommunication or Internet service provider's subscriber's records.

*How are other jurisdictions defining "traffic data"?*

The *Lawful Access* proposal does not define traffic data, although a number of other international statutory instruments do, including the *Convention*,<sup>93</sup> to which Canada is a signatory and the *G8 Tokyo Workshop 1*, in which Canada was a participant and principal drafter.<sup>94</sup>

<sup>89</sup> [2002] S.C.J. No. 59 at para. 168.

<sup>90</sup> 2002 SCC 10.

<sup>91</sup> *Ibid.* at para. 16.

<sup>92</sup> (1997) 147 D.L.R. (4th) 457 (SCC).

<sup>93</sup> *Convention*, *supra* note 20, Art. 1.

<sup>94</sup> In May 2001, the G8 held a high-level public-private workshop on cybercrime, which acknowledged the difficulty of defining "traffic data" and, while providing examples of the categories of data which could fall under the rubric, ultimately settled on the misleading definition of "not content" data. See G8, *Report on the Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service*

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

Under the *Convention*, traffic data means "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."<sup>95</sup>

The European Union *Directive on Privacy and Electronic Communications*<sup>96</sup> incorporates a broader, enumerated definition which includes latitude, longitude and altitude of the sender's or recipients terminal, direction of travel, identification of the network cell in which the terminal equipment is located at a certain point in time, any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection.

The U.K. *Regulation of Investigatory Powers Act*<sup>97</sup> (RIPA) contains a tortured, but relatively narrow definition of "traffic data" that includes subscriber and routing information and 'post-cut-through' data, or digits dialed after a call has been connected (i.e. your bank password if you use telephone banking services).<sup>98</sup> It also includes the data which is found at the beginning of each packet in a packet-mode network indicating which communications data attaches to which communication. The tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic data may identify a server but not a website or page.<sup>99</sup>

The U.S. *Communications Assistance for Law Enforcement Act*<sup>100</sup> (CALEA), uses the much narrower term "call-identifying information",<sup>101</sup> which means "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." The definition of "telecommunications carrier" excludes entities engaged in providing information services

---

*Providers*, (2001), online: <[http://www.mofa.go.jp/policy/i\\_crime/high\\_tec/conf0105-4.html](http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-4.html)> (date accessed: 15 Oct 2002).

<sup>95</sup> *Ibid.* at c. I, art. 1(d); for a plain illustration of the qualitative and quantitative differences in "traffic data" see A. Pascual, "Access to 'traffic' data: when reality is far more complicated than a legal definition" (Global Community Networks 2002, Montreal, 11 October 2002) [unpublished], online: <<http://www.it.kth.se/~aep/private/cnglobal2002-escuderoa.ppt>> (date accessed 19 Oct 2002).

<sup>96</sup> EC, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, [2002] O.J. L. 201 at para. 15.

<sup>97</sup> *Regulation of Investigatory Powers Act 2000* (U.K.), 2000, c. 23.

<sup>98</sup> *Ibid.* at s. 9.

<sup>99</sup> Explanatory Notes to *Regulation of Investigatory Powers Act 2000*, online: Home Office <<http://www.hmso.gov.uk/acts/en/2000en23.htm>> (date accessed: 15 Oct 2002).

<sup>100</sup> 47 U.S.C. §§ 1001-1010 (1994).

<sup>101</sup> *Ibid.* § 1001(2).



*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

(i.e. ISPs).<sup>102</sup> However, the FBI believes the CALEA guidelines apply to Internet and digital phone communications, and the U.S. Congress has favoured this interpretation in the *USA PATRIOT Act*.<sup>103</sup> The new law makes it clear that an order for a pen register or trap and trace applies to e-mail and Internet communications as well.

*The nature of information held in records is a factor in the contextual analysis for determining a reasonable expectation of privacy.*

Sopinka J., in *Branch*, was also careful to make a distinction between personal and business records: "documents produced in the course of a business which is regulated have a lesser privacy right attaching to them than do documents that are, strictly speaking, personal"<sup>104</sup>

The Court also found La Forest J.'s analysis in *Thomson Newspapers* helpful:

"While [business] records are not devoid of any privacy interest, it is fair to say that they raise much weaker privacy concerns than personal papers.... These records and documents do not normally contain information about one's lifestyle, intimate relations or political or religious opinions. They do not, in short, deal with those aspects of individual identity which the right of privacy is intended to protect from the overbearing influence of the state."<sup>105</sup>

In concluding that a lower expectation of privacy attached to business records, the Court in *Fitzpatrick* concluded that "the issue is buttressed by the fact that it cannot be said that using the information contained [in these records is] an affront to individual dignity - a fundamental value that underlies so many *Charter* rights. For these records divulge nothing about the personality of the individual who has created them. The information recorded is of a purely objective kind, and its relevance is limited entirely to a matter of importance only to the management and conservation of the fisheries. The information divulges nothing of the state of mind, thoughts, or opinions of the individual who has submitted the records."<sup>106</sup>

---

<sup>102</sup> *Ibid.* § 1001(8) "telecommunications carrier" ((A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire;... but (C) does not include (i) persons or entities insofar as they are engaged in providing information services...).

<sup>103</sup> *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001* is not a stand-alone statute, rather it amends 15 other acts, online: <[http://www.eff.org/Privacy/Surveillance/Terrorism\\_militias/20011025\\_hr3162\\_usa\\_patriot\\_bill.html](http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011025_hr3162_usa_patriot_bill.html)> (date accessed: 15 Oct 2002) (First it allows ISPs to voluntarily hand over all "non-content" information to law enforcement with no need for any court order or subpoena. s. 212. Second, it expands the records that the government may seek with a simple subpoena (no court review required) to include records of session times and durations, temporarily assigned network addresses (dynamic IP); means and source of payments, including credit card or bank account numbers. s. 210, 211.)

<sup>104</sup> *Ibid.* at para. 62.

<sup>105</sup> *Thomson Newspapers Ltd. v. Canada (Director of Investigation and Research, Restrictive Trade Practices Commission)*, [1990] 1 S.C.R. 425 at 517-18.

<sup>106</sup> *Fitzpatrick*, *supra* note 80 at para. 51.



*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

Thus, while production of records in the criminal context should always attract a higher judicial standard for invasions of privacy, Sopinka J. in *Baron v. Canada*, held that a label as to whether a statutory scheme is "regulatory" or "criminal" should not be determinative in deciding whether an unreasonable search or seizure is authorized: records produced for and under regulatory requirements may attract s. 8 protection.<sup>107</sup> Moreover, although business records generally attract a lower expectation of privacy than personal records, this is again not because of any label, but rather it is based on a contextual analysis of what these records typically contain and the purpose for which they were generated. This is consistent with the holding of the Court in *Dagg v. Canada (Minister of Finance)*,<sup>108</sup> which dealt with sign-in logs:

"In determining whether an individual has a reasonable expectation of privacy in a particular piece of information, it is important to have regard to the purpose for which the information was divulged. Generally speaking, when individuals disclose information about themselves they do so for specific reasons [and] they do not expect that the information will be... released to third parties without their consent."<sup>109</sup>

In *Plant* the Court found that computer records "revealing a pattern of electricity consumption in the residence could not reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence."<sup>110</sup> In *R. v. Johnston*,<sup>111</sup> counsel for the accused relied on *Plant* in arguing that a digital recording ammeter (DRA) was a much more invasive investigative tool than computerized consumption pattern records and that the information collected was of an intimate and private nature. The Court engaged a contextual analysis of the capabilities of the DRA to collect information and the nature of the information collected in finding that it was not an unreasonable invasion of privacy:

"[T]he police... witnesses for the Crown, along with the defence's witness... all confirm that one really cannot tell anything about what appliance a person may be using, if they are home at all, and if so, what they are doing. As Crown counsel indicated, a next-door neighbour or person on the street would likely have more information on what was going on in a house than the information obtained from the DRA. All it does is give a general graph of electrical use, and nothing more. In my view, this does not at all infringe on the privacy rights of an individual as contemplated by the *Charter* and as set out in *R. v. Plant*."<sup>112</sup>

Defence counsel and the court in *Johnston* properly relied on *Plant* as authority for the proposition that the interpretation of 'biographical core' must be on the basis that it is

<sup>107</sup> *Baron v. Canada*, [1993] 1 S.C.R. 416 at 444.

<sup>108</sup> [1997] 2 S.C.R. 403

<sup>109</sup> *Ibid.* at para. 75.

<sup>110</sup> [1993] 3 S.C.R. 281 at 293.

<sup>111</sup> [2002] A.J. No. 843.

<sup>112</sup> *Ibid.* at para. 6.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

permeable and infinite. Information can be outside the biographical core in one context and within it in another. The analysis of that in which an individual has a reasonable expectation of privacy must be a contextual one.

**Packet-mode communication intercepts are liable to massively infringe third-party Charter rights**

*Digital networks work differently than analog networks*

In traditional telecommunications, a telephone switch establishes a "circuit" between the caller and recipient, and that channel remains open during a call to carry information back and forth. By contrast, in "packet-mode" communication, information – voice or data – is broken down into small pieces of digital electronic information called "packets." Each packet is like an envelope, containing both message content and a header that indicates the point from which the packet originates and the point to which it is being sent. The header of a packet is analogous to a dialed number on a traditional telephone system; the message content is identical to the content of a telephone conversation. Each packet, containing a portion of the message, is transmitted individually and when all the packets reach their destination, they are reassembled into the complete message.<sup>113</sup>

Packet-mode communication is the transmission technology of the Internet. It is, moreover, becoming increasingly important for the transmission of voice conversations as well as data in modern telecommunications systems. The pace of digital convergence is accelerating, and packet-mode networks are fast becoming a more dominant feature of our telecommunications landscape.

*Investigatory tools for packet-mode communications cannot separate traffic and content data, necessitating a higher expectation of privacy for both.*

Packet-mode investigative tools suffer from overbroad application. Indeed, this is true of any rule-based system in a packet-mode environment, including web search engines and filtering software. The first difficulty is that divorcing "traffic data" from the content of the message is very difficult to do, if not impossible in a legal context; this issue is discussed elsewhere in these comments. Second, traffic data in digital networks is itself qualitatively and quantitatively 'richer' than that obtainable from traditional analog networks and will attract a higher expectation of privacy. The *Lawful Access* document seemingly ignores this fact and proposes the same or lower pre-authorization standards on the grounds that it is simply maintenance of lawful access capabilities;<sup>114</sup> this issue too is discussed elsewhere in these comments. Finally, rule-based systems are predicated on the ability to 'see' the target content and treat it according to pre-determined legal and

<sup>113</sup> *Communications Assistance for Law Enforcement Act* (Third Report and Order) (1999), CC Docket No. 97-213, FCC 99-230 (F.C.C.) at para. 55.

<sup>114</sup> *Lawful Access*, *supra* note 2 at 6 (this was also a common refrain heard at the civil society roundtables).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

technical parameters, however the underlying architecture of most digital networks precludes effective operation of this model. As Tim Berners-Lee, the inventor of the World-Wide Web, explains:

"There's a freedom about the Internet: as long as we accept the rules of sending packets around, we can send packets containing anything to anywhere..." The architecture of the network is designed to be "neutral with respect to applications and content. By placing intelligence in the ends, *the network has no intelligence to tell which functions or content are permitted or not....*"<sup>115</sup> [Emphasis added, footnotes omitted]

By requiring that the network itself remain neutral and open, with intelligence built into applications using the network, the underlying architecture has enabled extraordinary innovation, but has also made it extremely difficult to regulate content or even find and isolate it.<sup>116</sup> The U.S. Ninth Circuit Court of Appeals recently described this architecture as "end-to-end."<sup>117</sup> End-to-end disables central control over how the network develops and, as Industry Canada recently concluded, effectively precludes content-based determinations of acceptability.<sup>118</sup>

A recently disclosed internal FBI memo on the operation of Carnivore, a packet-mode, rule-based filtering system, indicates that this is real problem.

"The FBI software not only picked up the E-mails under the surveillance of the FBI's target... but also picked up E-mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-mail take, including the take on..."<sup>119</sup>

The author of the memo states:

"The software was turned on and did not work correctly."

In fact, it *was* working correctly, but packet-mode rule-based filters suffer from congenital inaccuracy and are liable to massive invasions of privacy of innocent third-party subscribers not because of the nature of the tool or technique so much as the

<sup>115</sup> Lessig, *supra* note 10 at 40.

<sup>116</sup> G. Miller et al. *Regulation of the Internet: A Technological Perspective*, (1999), online: Industry Canada <[http://strategis.ic.gc.ca/SSU/sf/005082\\_e.pdf](http://strategis.ic.gc.ca/SSU/sf/005082_e.pdf)> (last modified: March 1999) at 3 [Miller]; see also Digital Copyright Reform, *supra* note 12.

<sup>117</sup> *AT&T v. City of Portland*, 216 F.3d 871, 879 (9<sup>th</sup> Cir. 2000) ("The Internet's protocols themselves manifest a related principle called "end-to-end": control lies at the ends of the network where the users are, leaving a simple network that is neutral with respect to the data it transmits, like any common carrier."). The phrase comes from the work of network architects J. Saltzer *et al.*, "End to End Arguments in System Design", *ACM Transactions in Computer Systems* 2 at 277-288 (4 November 1984).

<sup>118</sup> Miller, *supra* note 116 at 3.

<sup>119</sup> FBI Memo on errors in *Foreign Intelligence Service Act* intercepts using FBI Internet monitoring system, Carnivore, at <http://www.epic.org/privacy/carnivore/fisa.html>.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on  
Lawful Access*

environment in which they will be employed.<sup>120</sup> Notwithstanding technological development of new investigatory tools, surveillance by these means will always be liable to inaccuracy in targeting and collecting only that information which may be relevant to a given person. This can best be explained by way of illustration.

An Illustration of the (In)Accuracy of a Packet-Mode Filter

Let us assume that one person out of a 100,000 is a terrorist and communicating evidence of such over the network. Law enforcement installs a filter at a service provider that is designed to trap all packets that may be of interest to an anti-terrorism investigation. The filter or "packet-sniffer", as it is commonly-known, traps only packets described by specific, target parameters and is 99.999% accurate in its task – if a packet contains evidence of terrorism, the filter has a 99.999% chance of identifying it as such and an 0.001% chance of erring and identifying the packet as innocent. Similarly, if a packet is innocent, the filter has a 99.999% chance of saying so, and an 0.001% chance of incorrectly flagging it as evidence of terrorism. For the sake of simplicity, we will also assume that each subscriber only sends or receives one packet per day (in reality, the average Internet subscriber probably sends or receives approximately one million packets per day, but this would make the calculations unwieldy for our purposes).

If one packet in 100,000 actually does contain evidence of terrorism, what happens? The filter will almost certainly catch that one packet. It will also tag 0.001% of innocent packets – which also works out to almost exactly one per 100,000. Of the packets tagged by the filter, half are innocent. Since packets equal people in our illustration, the filter will finger one innocent person for every terrorist. An accuracy rate of 50%.

To be precise with the numbers:

1 in 100,000 guilty packet/person = 0.00001 per 1 input  
99,999 innocent packet/people = 0.99999 per 1 input  
Flag 99.999% of guilty packets/people » catch (correctly) 0.000099999 per 1 input  
Flag 0.001% of innocent packets/people » false positives 0.000099999 per 1 input  
They are equal, so it is trivial that the result is 50/50.

For a slightly less accurate (and more realistic) filter:

1 in 100,000 is a guilty packet/person = 0.00001 per 1 input  
99,999 are innocent packets/people = 0.99999 per 1 input  
Flag 99.99% of » catch (correctly) 0.00009999 per 1 input  
Flag 0.01% of innocent » false positives 0.00099999 per 1 input  
Total flagged » 0.00009999+0.00099999 = 0.00109998 per 1 input

<sup>120</sup> Needs Assessment, *supra* note 8 at 33 (31% of investigators identified the inability to selectively monitor traffic as a problem they encountered at least often, compared to only 22% who said they had never encountered this problem).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

How much of flagged traffic is innocent?

$$0.00099999 \div 0.00109998 = 0.9090983472 = \sim 91\%$$

How would we feel about a system in which almost all guilty persons were charged, but where 91% of those charged were innocent? In 2001, Bell Canada had in excess of 1.5 million Internet subscribers and 2.9 million wireless subscribers.<sup>121</sup> Using the above model, 150 innocent Bell Canada Internet subscribers and 290 wireless subscribers would have been marked as terrorists in 2001.

*Massive infringements of third-party Charter rights can be determinative of constitutionality*

In *R. v. Thompson*, the Supreme Court considered whether the extent of a invasion of a third-party's rights could be determinative of constitutionality for the second stage of a s. 8 analysis, namely the unreasonableness of the search.

"[A] potentially massive invasion of... privacy" of members of the general public who were not involved in the suspected criminal activity... cannot be ignored simply because it is not brought to the attention of the court by one of those persons. Since those persons are unlikely to know of the invasion of their privacy, such invasions would escape scrutiny, and s. 8 would not fulfill its purpose."<sup>122</sup>

While this may sometimes be "justified in appropriate circumstances" as Sopinka J. observed in *Thompson*, it would seem corollary and common-sense that if a technique was liable for massive infringement that it would attract the very highest *ex ante* scrutiny and not the reverse, as the Department of Justice proposes in the Lawful Access Consultation document.

La Forest J., for the majority in *Duarte*, opined:

"[I]f the surreptitious recording of private communications is a search and seizure within the meaning of s. 8 of the *Charter*, it is because the law recognizes that a person's privacy is intruded on in an unreasonable manner whenever the state, *without a prior showing of reasonable cause* before a neutral judicial officer, arrogates to itself the right surreptitiously to record communications that the originator expects will not be intercepted by anyone other than the person intended by its originator to receive them...."<sup>123</sup> [Emphasis added]

This prophylactic interpretation of s. 8 has found effective expression in the judicial preauthorization requirement developed by Dickson J. in *Hunter*:

<sup>121</sup> Bell Canada Financial Information 2001, Annual Report, (April 16, 2002) at 2 "Operational Highlights".

<sup>122</sup> *Thompson*, *supra* note 74 at 1143.

<sup>123</sup> *Duarte*, *supra* note 60 at para. 28.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

"[The] purpose [of s. 8 is] to protect individuals from unjustified state intrusions upon their privacy. That purpose requires a means of *preventing* unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place. This, in my view, can only be accomplished by a system of *prior authorization*, not one of subsequent validation."<sup>124</sup> [Emphasis in original]

Section 8 would have very little value as a guarantee to the right to privacy if it operated only to exclude, *ex post facto*, information obtained in an unreasonable manner; by that time, the individual's privacy has already been violated and the personal and intimate information is in the hands of the authorities.<sup>125</sup>

**Diluted judicial standards grant too much subjective discretion to individual law enforcement officers.**

The requirement that law enforcement first seek independent judicial authorization for warrants serves as a check against the unfettered discretion of individual law enforcement officers and creates a record of accountability subject to audit of abuse and defects in the law.

Under the *Highway Traffic Act* in Ontario, and similar statutes in other provinces, the standards for search and seizure have been diluted in ways similar to that now proposed by the Department of Justice. A discussion of the policy, jurisprudence and social commentary relating to investigatory detentions can help stakeholders chart future directions in the lawful access debate.

*Driving lessons: what can we learn from lower judicial standards for investigations under the Highway Traffic Act and similar statutes?*

In 1977, the Etobicoke Police Service implemented an anti-drinking and driving campaign called "Reduce Impaired Driving in Etobicoke" ("R.I.D.E."). The program required police to establish strategic, stationary checkpoints to screen passing motorists for alcohol consumption. Officers screened randomly or on the belief that a motorist might be impaired. Any person refusing a screening test could be detained and subject to criminal sanctions.

The dilution of probable cause under the R.I.D.E. program was mitigated, to an extent, by its high-visibility and by its more or less equal application to all motorists transiting stationary checkpoints. Even if the ultimate decision to screen one motorist and not another was made by a single officer exercising his or her own personal biases, that

<sup>124</sup> *Hunter*, *supra* note 62 at 160; for a discussion of the exclusionary rule under the 4<sup>th</sup> Amendment, see D. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy" (2002) 75 *S. Cal. L. Rev.* 1083.

<sup>125</sup> *Schreiber v. Canada (Attorney General)*, [1998] 1 S.C.R. 841 at para. 46.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

officer's conduct "can be observed by other officers. Since he [or she] has limited time to observe a vehicle, his [or her] decision will be either truly random or based on some objective basis. The result is that this method of enforcement is somewhat more carefully designed to serve enforcement, less intrusive, and not as open to abuse as [a roving random stop]."<sup>126</sup> Today, the R.I.D.E. program has been expanded across Ontario and into other Canadian jurisdictions.<sup>127</sup> Importantly, it no longer operates under the same organized procedures.

Section 48 of Ontario's *Highway Traffic Act*,<sup>128</sup> authorizes law enforcement to stop any motorist at any time to determine "whether or not there is evidence to justify making a demand [for a breathalyzer analysis]". A police officer need not satisfy any other grounds – or any objective criteria at all – in order to stop a motorist and subject him or her to a screening test. Similarly, on its face s. 216(1) of the *Act* grants police officers authority to stop motor vehicles for any lawful reason related to the enforcement of laws relating to motor vehicle use.

Under s. 48 and s. 216(1) of the *Act* in Ontario and similar provisions in other provincial statutes throughout Canada, police officers can conduct random roving stops of motorists anywhere and at anytime. There is no need for law enforcement to justify a stop nor can judicial oversight be effective because there is no objective criteria against which a judge can measure an officer's belief that such action was justified. In *Ladouceur*, Sopinka J. observed the flaw in this formula: "If... no reason need be given or is necessary, how will we ever know [if a stop violates the *Charter*]? The officer need only say, "I stopped the vehicle because I have the right to stop it for no reason. I am seeking unlicensed drivers."<sup>129</sup>

In *R. v. Hufsky*,<sup>130</sup> Le Dain J., writing for a unanimous Supreme Court, held that random stops conducted under an organized "spot check" program and authorized by the *Highway Traffic Act* did not violate the *Charter*. The Court concluded that, although the random stop constituted arbitrary detention in violation of s. 9 of the *Charter*, it was justified under s. 1 in view of the importance of highway safety. The Court also held that the random stop did not constitute an unreasonable search and seizure in violation of s. 8 of the *Charter*.<sup>131</sup>

<sup>126</sup> Sopinka J. concurring in result, *R. v. Ladouceur*, *infra* note 132 at para. 10.

<sup>127</sup> In British Columbia, the equivalent program, established in 1984, is known as "Drinking Driving Counterattack".

<sup>128</sup> R.S.O. 1990, c. H.8, s. 48(1).

<sup>129</sup> *Ladouceur*, *infra* note 132 at para. 11. Sopinka J. concurred in the result, but not the reasons for judgment. See also A. Young, "All Along the Watchtower: Arbitrary Detention and the Police Function" (1991) 29 Osgoode Hall L. J. 329 at n. 49 and accompanying text (describing the operation of General Order 304.10 by the D.C. Metro Police which required the documentation of "contacts" and "stops" in an effort to make police more accountable for their interaction with members of the public, particularly visible-minorities) [Watchtower].

<sup>130</sup> [1988] 1 S.C.R. 621 at para. 23.

<sup>131</sup> In the United States, vehicle and "stop-and-frisk" or "Terry" stops are scrutinized under the search and seizure provisions of the Fourth Amendment. Canada deals with investigative detentions under s. 9 of the *Charter*, which provides that, "[e]veryone has the right not to be arbitrarily detained or imprisoned." The lawfulness of this type of detention has been recognized and limited in Canada by the Ontario Court of

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

*Subjectively-based assessments can too easily mask discriminatory conduct*

In *R. v. Ladouceur*,<sup>132</sup> the Supreme Court expanded the *Hufsky* doctrine in finding that a routine but otherwise "purely random" check under the *Highway Traffic Act* was an arbitrary detention in violation of s. 9 of the *Charter*, but was reasonably and demonstrably justified in a free and democratic society under s. 1. The officers had no basis of suspicion and no other reason to stop the appellant, but the Court held the power should be justified because the *Act* dealt with a pressing and substantial concern (*i.e.* highway safety), the random check was the only effective deterrent, and it impaired the s. 9 right as little as possible. Although all nine judges of the Court concurred in the result, the minority of four recognized that unlimited police discretion to stop was problematic and for those reasons would have sided with the Ontario Court of Appeal in deciding that the *Act* should be interpreted as being limited "to an organized programme of stopping, like the R.I.D.E. programme, or road-blocks where all vehicles are required to halt, or [stop] for some articulable cause."<sup>133</sup>

Three years later the Ontario Court of Appeal, in *R. v. Simpson*,<sup>134</sup> narrowed the effective application of *Ladouceur* in finding that an officer's purpose for stopping a vehicle for "purely investigative purposes" unrelated to the enforcement of laws relating to the operation of motor vehicles was not lawful and was not justified on the facts because the detaining officers lacked "articulable cause" for the detention. In justifying the "articulable cause" standard in *Simpson*, Doherty J.A. wrote:

"These cases require a constellation of objectively discernible facts which give the detaining officer reasonable cause to suspect that the detainee is criminally implicated in the activity under investigation.... A "hunch" based entirely on intuition gained by experience cannot suffice, no matter how accurate that "hunch" might prove to be. Such subjectively based assessments can too easily mask discriminatory conduct based on such irrelevant factors as the detainee's sex, colour, age, ethnic origin or sexual orientation."<sup>135</sup>

In *Brown v. Durham Regional Police Force*<sup>136</sup> the court considered that a stop may be lawful under s. 216 of the *Highway Traffic Act* even if it is made for purposes other than

---

Appeal in *R. v. Simpson*, *infra* note 134 and subsequently in the Courts of Appeal of Alberta, Saskatchewan, Newfoundland, Manitoba, Nova Scotia and Québec: *R. v. Dupuis* (1994), 162 A.R. 197 (Alta. C.A.); *R. v. Lake* (1996), 113 C.C.C. (3d) 208 (Sask. C.A.); *R. v. Burke* (1997), 118 C.C.C. (3d) 59 (Nfld. C.A.); *R. v. G. (C.M.)* (1996), 113 Man. R. (2d) 76 (Man. C.A.); *R. v. McAuley* March 26, 1998, AR97-30-03243, AR97-30-03328 [reported (1998), 124 C.C.C. (3d) 117 (Man. C.A.)]; *R. v. Chabot* (1993), 86 C.C.C. (3d) 309 (N.S. C.A.); *R. c. Pigeon* (1993), 59 Q.A.C. 103 (Que. C.A.).

<sup>132</sup> [1990] 1 S.C.R. 1257.

<sup>133</sup> *Ibid.* at para. 13.

<sup>134</sup> (1993), 12 O.R. (3d) 182.

<sup>135</sup> *Ibid.* at para. 61.

<sup>136</sup> (1998), 138 C.C.C. (3d) 1 (Ont. C.A.).



*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

those related to highway safety matters provided that these other purposes are not themselves improper. Doherty J.A. directly addressed the concern raised in this case:

"While I can find no sound reason for invalidating an otherwise proper stop because the police used the opportunity afforded by that stop to further some other legitimate interest, I do see strong policy reasons for invalidating a stop where the police have an additional improper purpose.... Officers who stop persons intending to conduct unauthorized searches, or who select persons to be stopped based on their sex or colour, or who stop someone to vent their personal animosity toward that person, all act for an improper purpose."<sup>137</sup>

To a greater degree than in Canada, courts and commentators in the United States have acknowledged that unlimited police discretion to stop and search will result in the harassment of disfavored racial or cultural minorities or be used as a pretext for investigation of unrelated criminal activity. These assumptions are strongly supported by social science research, literature and media reports.<sup>138</sup>

In 1979, in *Delaware v. Prouse*,<sup>139</sup> a motorist challenged the constitutionality of a "random spot check" procedure under which state patrol officers could stop a motorist without probable cause to check the validity of the vehicle's registration or the driver's license.

In ruling in the motorist's favor and striking down the practice, the Court considered social science data suggesting that unbridled discretion would lead law enforcement officers to stop individuals on the basis of "salient cues" such as race. The data demonstrated the tendency of officers to use their discretionary power to conduct stops, interrogations, and searches of people who are "different" from the racial majority and, more importantly, different from the police officers themselves. Echoing this sentiment in Canada, the Supreme Court in *R. v. Landry* noted that "abuses of police power will rarely affect respectable members of the middle classes," but will instead "focus upon the poor and on the marginal, minority groups."<sup>140</sup>

In the more recent case of *Whren v. United States*,<sup>141</sup> the petitioner cited anecdotal evidence that police officers disproportionately target people of color for traffic stops and requests for consent to search. While acknowledging the difficulties of substantiating the claim of racial motivation given that police departments often fail to document their stops, the petitioner pointed to patterns of police conduct in Florida, Pennsylvania, and Colorado that demonstrate the disproportionate frequency with which officers stop motorists of color.<sup>142</sup> Former Osgoode Hall law professor, Alan Young, observed that

---

<sup>137</sup> *Ibid.* at 17.

<sup>138</sup> A. Thompson, "Stopping the Usual Suspects: Race and the Fourth Amendment" (1999) 74 *N.Y.U. L. Rev.* 956 at 974.

<sup>139</sup> 440 U.S. 648 (1979).

<sup>140</sup> *R. v. Landry* (1986), 25 C.C.C. (3d) 1 at 30 (S.C.C.).

<sup>141</sup> 517 U.S. 806 (1996).

<sup>142</sup> *Whren v. United States*, 517 U.S. 806 (1996) (No. 95-5841) (Brief for Petitioners at 18-19).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

"we have yet to recognize that vast discretionary powers are exercised by the police that do not ever crystallize into a formal arrest or the laying of a charge."<sup>143</sup>

In Toronto, a police board of inquiry, in dismissing a complaint brought against an officer, found that two black men on their way home from work appeared suspicious when they stared "intently" at a marked police car.<sup>144</sup> This suspicious behaviour was enough to justify a stop of the vehicle and a high-risk takedown of its occupants neither of whom were ultimately arrested. The complaint and appeal were dismissed,<sup>145</sup> as was a conduct hearing, which nonetheless observed that while the Board of Inquiry was aware of the "perception held by some members of the public that black motorists are randomly and arbitrarily stopped by police officers for no reason other than the colour of their skin," it was satisfied that the officers' conduct was warranted in light of the "suspicious activity" of the complainant's vehicle.<sup>146</sup>

The Board's ethereal 'public perception' materialized into hard numbers recently in an analysis of Toronto arrest statistics by *The Toronto Star*. Information from the Criminal Information Processing System, a database of all arrests made by Metro Toronto police, proves that police ticket a disproportionate number of blacks for violations that routinely surface only after a stop has been made. In the absence of any other charge, it isn't clear why drivers involved in these offences were stopped in the first place.<sup>147</sup>

*Discrimination is a corollary of discretion, not a synonym for racism.*

It is now beyond debate that police discretion is often exercised on a racial and class basis.<sup>148</sup> The police exercise their discretion in a manner that targets those who appear out of place or different from the police themselves; this determination is premised upon race, socio-economic status and stereotyping. It is said that "officers look for and employ status cues to determine what action they should take; in this sense, 'police activity is as much directed to who a person is as to what he does.'"<sup>149</sup>

<sup>143</sup> Watchtower, *supra* note 129 at 341.

<sup>144</sup> *Ontario v. Hannah* (1997), 145 D.L.R. (4th) 443 at 445 (Ont. Gen. Div. (Div. Ct.)).

<sup>145</sup> D. Tanovich, "Using the Charter to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention" (2002) 40 *Osgoode Hall L.J.* 145 at 155-57.

<sup>146</sup> P. Mascoll, "Police Cleared In 'Take Down'" *The Toronto Star* (27 September 1995) A1.

<sup>147</sup> See e.g. "Police Target Black Drivers" *The Toronto Star* (Oct 20 2002); See also "The Story Behind the Numbers" *The Toronto Star* (19 Oct 2002); "Treatment Differs By Division" *The Toronto Star* (Oct 19 2002).

<sup>148</sup> R. Harper, "Has the Replacement of Probable Cause with Reasonable Suspicion Resulted in the Creation of the Best of All Possible Worlds" (1988) 22 *Akron L. Rev.* 13 at 38. ("Research suggests that while the police do tend to detain and arrest blacks at a higher rate than they do whites with whom they come in to [sic] contact, it is probable that race, in itself, is not the explanatory factor. It is more likely that poverty and low socio-economic status, with which race tends to be associated, figure more importantly into the police detention and arrest decision. It is thus in poorer neighbourhoods, where the police presence is likely to be greater, where the citizens' demeanour toward the police may be interpreted as offensive, and where the people with whom the police interact generally lack resources and other indicia of social power, that the police are less likely to refrain from stopping citizens for investigation." See also S. Johnson, "Race and the Decision to Detain a Suspect" (183) 93 *Yale L.J.* 214.

<sup>149</sup> Watchtower, *supra* note 129.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

According to former Harvard Business School professor, Renato Tagiuri, we cluster information into categories and this leads inevitably to some prejudgment based upon our perceptions of those groupings. Stereotypes have been defined as the "general inclination to place a person in categories according to some easily and quickly identifiable characteristic such as age, sex, ethnic membership, nationality, or occupation, and then to attribute to him qualities believed to be typical of members of that category."<sup>150</sup> Of course, stereotypes about groups tend not to be any more accurate than any other type of generalization<sup>151</sup> because they represent oversimplification of complexities. But we tend to rely on them and, at times, to be prejudiced by them in making complex discretionary decisions.

In a study of video surveillance use by police in the United Kingdom, Dr. Clive Norris and Gary Armstrong of the Centre for Criminology and Criminal Justice at Hull University found that "the gaze of the cameras do not fall equally on all users of the street but on those who are stereotypically predefined as potentially deviant, or through appearance and demeanor are singled out by operators as unrespectable. In this way youth, particularly those already socially and economically marginal, may be subject to even greater levels of authoritative intervention and official stigmatization, and rather than contributing to social justice through the reduction of victimization, [surveillance] will merely become a tool of injustice through the amplification of differential and discriminatory policing."<sup>152</sup>

State intrusion in the name of law enforcement has a tendency to expand into social control of groups perceived to be deviant or marginalized. history of s"[T]he history of street powers... demonstrates that the traditional practices of law enforcement on the streets have had very little connection with crime *per se* and a great deal to do with social control of the urban populace."<sup>153</sup>

<sup>150</sup> R. Tagiuri, "Person Perception" in G. Linzey & E. Aronson, eds., *Handbook of Social Psychology*, 2<sup>nd</sup> ed. (New York: Random House, 1985).

<sup>151</sup> See R. Spears, "From personal pictures in the head to collective tools in the world" in C. McGarty et al., eds., *Stereotypes as explanations: the formation of meaningful beliefs about social groups*, (London: Cambridge University Press, 2002) (shared stereotypes allow groups to represent and change social reality); B. Wittenbrink et al., "Structural properties of stereotypic knowledge and their influences on the construal of social situations" (1997) 72(3) *J. of Personality & Social Psych.* 526-543 (stereotypic assumptions about cause-effect relations provide important constraints for the causal structure underlying the perceiver's subjective representation of social information).

<sup>152</sup> C. Norris and G. Armstrong, "The Unforgiving Eye: CCTV Surveillance in Public Spaces" (1998) at 8.

<sup>153</sup> M. Brogden, "Stopping the People – Crime Control Versus Social Control" in J. Baxter and L. Koffman, eds., *Police: The Constitution and the Community* (Abingdon, U.K.: Professional Books, 1985) at 106.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

*Diluted judicial standards encourage prejudicial subjective-assessment by law enforcement which could lead to the de facto offence of "Surfing While Muslim"... or while being political... or of being a teenager... or of being a part of stereotyped group...*

The Supreme Court has justified diluted judicial standards for investigative detentions under the Ontario *Highway Traffic Act* and equivalent statutes in other provinces on the grounds that highway safety poses a reasonable and justifiable limit on s. 9 and s. 8 rights under the *Charter*. However, time and increased public attention have raised important considerations regarding the lack of objective criteria for investigative detentions. First, diluted judicial standards encourage individual police officer's to make subjectively-based assessments which can too easily mask discriminatory conduct. This has been widely acknowledged by U.S. courts, in academic literature, social science data and the media on both sides of the border. Second, lower standards preclude effective judicial and public oversight of possible *Charter* violations.

Following on the heels of their American counterparts, Canadian courts have more recently acknowledged that the diluted standards are problematic and have sought to read down discretionary powers.

The *Lawful Access* document proposes diluted judicial standards for investigatory powers under the *Criminal Code* and other statutes and, in so doing, ignores the lessons learned in the investigative detention context above.<sup>154</sup> Why should we expect that diluted judicial standards as applied to the Internet will be any less discriminatory simply because we are driving on an information highway? Indeed, we should expect that they would be more so for the reasons already discussed elsewhere in these comments, namely that: 'traffic data' and 'content data' are difficult to divorce from each other such that the act of "stopping" a packet is the same as searching it; and, also that when you "stop" one target packet, there is a high-probability that you will "stop" unintended packets along with it.

Moreover, diluted judicial oversight and the natural predilection of even the most fair-minded person to prejudge their perceptions has, in the context of investigative detentions of drivers, led down a slippery slope of subjectivity that many Black North Americans euphemistically call "DWB", the offence of "Driving While Black".<sup>155</sup>

Discretion is the hallmark of individualized justice but it can just as easily contain the seeds of inequity. Without procedural safeguards, discretion will often be exercised in a manner not consonant with the goals and spirit of valid legislative objectives and legal control becomes a more all-embracing form of social control.

<sup>154</sup> *Lawful Access*, *supra* note 2 at 11 (claiming production orders "less invasive", contemplating lower expectation of privacy in traffic data), 12 (interpreting *Plant* to suggest that some types of data should not require judicial authorization).

<sup>155</sup> See D. Harris, *Driving While Black: Racial Profiling On Our Nation's Highways* (Special Report) (New York: ACLU, 1999), online: ACLU <<http://www.aclu.org/profiling/report>> (date accessed: 9 Nov 2002); K. Meeks, *Driving While Black: Highways, Shopping Malls, Taxicabs, Sidewalks: How to Fight Back if You are a Victim of Racial Profiling* (New York: Broadway Books, 2000); G. Webb, "DWB" *Esquire* 131:4 (April 1999) 118.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

In the present political atmosphere and in the context of the *Lawful Access* proposal, it does not take much foresight or even creativity to interpolate 'driving' with 'surfing' and 'Black' with 'Muslim' to imagine that diluted judicial scrutiny could lead to a new cyber-offence, in Canada, of "Surfing While Muslim". Salient interests could include a Muslim-sounding name, an IP address from an Arab country or organization, an online purchase of the most recent book by author Youssef Samir, Salman Rushdie or any number of others as defined by the personal biases of the individual investigator. Similar discretion could later be applied to any number of groups frequently stereotyped as exhibiting undesirable behaviour, including youths and various political causes.

**Conclusion:** applying traditional rules of lawful access to the persistent, pervasive and permanent information realm of cyberspace, is not simply a maintenance of the *status quo*, but rather introduces new and unique implications for privacy and freedom of expression.

The *Lawful Access* document and consultation have failed to provide any meaningful justification for the proposed expansion of powers, save to suggest that Canada has an international obligation to adopt the *Convention*, that the amendments are merely technical, and that the purpose of the initiative is simply to maintain the *status quo*.

The proposed amendments in the *Lawful Access* document would have the effect of moving criminal investigations away from carefully constructed standards of reasonable and probable cause – that an investigator has sufficient grounds to believe that a *specific* person has committed or is likely to commit an offence – towards the general proposition that everyone is potentially of interest simply for 'driving on the information highway'.

There is little doubt that new information and communications technologies are impeding traditional investigations of crime, including online crime. Moreover, it is uncontested that at some point in the near future, we may see new kinds of *sui generis* cybercrime – identity theft is the first portent of this – which may require the articulation of different legal standards. At present, cybercrime is little more than conventional crime by unconventional means. Unlike highway safety legislation which permits reduced judicial oversight for investigation related to highway safety, the argument that new legal standards are required to effectively combat cybercrime is not rationally connected to promoting safety or ameliorating a well-defined and serious social problem.

Stanford law professor, Lawrence Lessig, has observed that more than law alone enables legal values, and law alone cannot guarantee them.<sup>156</sup> In cyberspace, and in cybercrime investigations, frequently code and technical standards are as important as law. The *Lawful Access* document claims that technology lies at the root of many of the difficulties now faced by law enforcement and national security agencies in their efforts to investigate and prosecute crime in cyberspace. The Dartmouth needs assessment supports the conclusion that improved *technological* and *administrative* solutions would

<sup>156</sup> L. Lessig, "The Law of the Horse: What Cyberspace Might Teach" (1999) 113 *Harv. L. Rev.* 501.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

substantially address the public policy objectives of lawful access. The author suggests that a holistic approach to the impediments of cybercrime investigation and prosecution will be more effective than the approach now emphasized in the *Lawful Access* document. Further, such an approach would have less of an impact on Canadians' constitutional rights and freedoms.

The government recognizes the importance of code-as-law to the degree that it seeks to compel telecommunications and Internet service providers to provide the technical capability for lawful access, but fails to factor it into the consideration of the standard for access to traffic data. In many instances, traffic data will reveal as much if not more about one's lifestyle, intimate relations or political or religious opinions as content data. Canadian courts have determined that such information attracts a high reasonable expectation of privacy, particularly in the criminal investigation context. Further, the line between traffic and content will only become more blurred as Canadians expand their daily activities into cyberspace, providing increased opportunities for linkages between formerly discrete aspects and transitory bits of individual lives.

Similarly, the government fails to consider the implications that increased individual discretion under a diluted judicial oversight standard will have on *Charter* rights in cyberspace. Investigation is a legitimate and necessary police power, but efforts must be made to ensure it does not blossom into a form of panoptic surveillance.

We cannot afford to wait to vindicate privacy only after it has been violated; this is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated. The factual foundation of 'reasonable and probable' grounds that an offence has been or will be committed is not only a safeguard against unfettered individual discretion, but it creates a record of accountability subject to audit of abuse of authority and inevitable defects in the law.

The *Lawful Access* proposals have grave implications for privacy and freedom of expression in Canada. The conclusion we cannot fail to reach is that applying traditional rules of lawful access to the realm of cyberspace is, in fact, not simply maintaining the *status quo*.

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

**Appendix A: Traffic Data**<sup>157</sup>

*Traffic data on a plain old telephone system (POTS)*

20021021070824178 165 0187611205 6139574222 -----001-----003sth 46 5145281768-----0013  
1410260

Caller at (613) 957-4222 makes a phone call at 7:08:24 AM on October 21, 2002 to recipient at (514) 528 1768 for 3 minutes and 20 seconds.

*Traffic data from plain old telephone service (POTS) line to an ISP (dial-up)*

Fri Oct 19 11:30:40 2001  
User-Name = "aep@somedomain.org"  
NAS-IP-Address = 62.188.74.4  
NAS-Port = 3239  
NAS-Port-Type = Async  
Acct-Status-Type = Start  
Acct-Delay-Time = 0  
Acct-Session-Id = "324546354"  
Acct-Authentic = RADIUS  
Calling-Station-Id = "6139574222"  
Called-Station-Id = "5145281768"  
Framed-Protocol = PPP  
Framed-IP-Address = 62.188.17.227  
Proxy-State "PX01\0\0\0xcdntg\0x13\0xdfV\0xa4\[\...\0xfc\0x8c"

On Friday, October 19<sup>th</sup> 2001 at 11:30:40 AM, Internet subscriber aep@somedomain.org at IP address 62.188.17.227 calling from (613) 957-4222 in Ottawa places a 21 second call using an asynchronous modem to (514) 528-1768 in Montréal.

*Traffic data from two callers on a wireless network (~GSM)*

time GMT=20010810010852 Cell ID=115 MAC ID=00:02:2D:20:47:24 (A)  
time GMT=20010810010852 Cell ID=115 MAC ID=00:02:2D:04:29:30 (B)  
time GMT=20010810010852 Cell ID=115 MAC ID=00:60:1D:21:C3:9C  
time GMT=20010810010853 Cell ID=129 MAC ID=00:02:2D:04:29:30  
time GMT=20010810010854 Cell ID=129 MAC ID=00:02:2D:1F:53:C0  
time GMT=20010810010854 Cell ID=129 MAC ID=00:02:2D:04:29:30 (B)  
time GMT=20010810010854 Cell ID=129 MAC ID=00:02:2D:20:47:24 (A)  
time GMT=20010810010856 Cell ID=41 MAC ID=00:02:2D:0A:5C:D0  
time GMT=20010810010856 Cell ID=41 MAC ID=00:02:2D:1F:78:00  
time GMT=20010810010900 Cell ID=154 MAC ID=00:02:2D:0D:27:D3

<sup>157</sup> Adapted from A. Pascual, "Access to 'traffic' data: when reality is far more complicated than a legal definition" (Global Community Networks 2002, Montreal, 11 October 2002) [unpublished], online: <<http://www.it.kth.se/~aep/private/cnglobal2002-escuderoa.ppt>> (date accessed 19 Oct 2002).

*Comments submitted in consideration of the Cyber-crime Convention and the Consultation Paper on Lawful Access*

On August 10, 2001 at 1:08:52 AM, cellphone user A was in radio cell 115 (Dorval Airport) with cellphone user B and both traveled together at 01:08:54 am to cell 129 (Hilton Hotel).

*Traffic data from a user connecting to a web server*

295.47.63.8 - - [05/Mar/2002:15:19:34 +0000] "GET/cgi-bin/htsearch?config=htdigx&words=startrek HTTP/1.0"20 2225  
295.47.63.8 - - [05/Mar/2002:15:19:44 +0000] "GET/cgi-bin/htsearch?config=htdig&words=startrek+avi HTTP/1.0"200x  
215.59.193.32 - - [05/Mar/2002:15:20:17 +0000] "GET/cgi-bin/htsearch?config=htdig&words=Modem+HOWTO ...  
192.77.63.8 - - [05/Mar/2002:15:20:35 +0000] "GET/cgi-bin/htsearch?config=htdig&words=conflict+war HTTP/1.0"200  
211.164.33.3 - - [05/Mar/2002:15:21:32 +0000] "GET/cgi-bin/htsearch?config=htdigx&words=STD+clinic+Kingston...  
211.164.33.3 - - [05/Mar/2002:15:21:38 +0000] "GET/cgi-bin/htsearch?go=1&do=nw&ct=NA&ly=US&la=1234+Main+Street  
&lp=&lc=Kingston&ls=ON&lz=K7L+3H4&lah=&2y=US&2a=300+1st+Avenue&2p=&2c=Kingston  
&2s=ON&2z=K4E+4T5&2ah=&lr=2&x=83&y=10  
211.164.33.3 - - [05/Mar/2002:15:22:05 +0000] "GET/cgi-bin/htsearch?config=htdigx&words=taxi+info  
82.24.237.98 - - [05/Mar/2002:15:25:29 +0000] "GET/cgi-bin/htsearch?config=htdigx&words=blind+date HTTP/1.0

On March 5<sup>th</sup> 2002, Internet surfer at IP 211.164.33.3 searches for information on Kingston STD clinics, driving directions from 1234 Main St., Kingston, ON K7L 3H4 to 300 1<sup>st</sup> Avenue, Kingston, ON K4E 4T5 and taxi info.



**Pierlot, Paul**

**From:** [REDACTED]  
**Sent:** 2002 Dec 16 4:20 PM  
**To:** 'la-al@justice.gc.ca' s.19(1)  
**Cc:** [REDACTED]  
**Subject:** Lawful Access - Consultation Document - RWI Comments



Lawful Access Dec 16  
Letter.pdf...



Lawful Access Dec 16  
Comments....

**ELECTRONIC FILING SUMMARY:**

2002/12/16 - Rogers Wireless Inc.  
Lawful Access - Consultation Document  
DESCRIPTION: Letter to Industry Canada

**FILE NAMES:**

Lawful Access Dec 16 Letter.pdf - 30 KB (Adobe Document)  
Lawful Access Dec 16 Comments.pdf - 158 KB (Adobe Document)

<<Lawful Access Dec 16 Letter.pdf>> <<Lawful Access Dec 16 Comments.pdf>>

If you have any problems accessing the attached, please call [REDACTED] at 416-935-7212.

\*\*\*\*\*  
\*\*\*\*\*

This email may contain privileged, confidential or undisclosed information. If the reader of this email is not the intended recipient or an agent responsible for delivering it to the intended recipient, you are hereby notified that you have received this email in error, and that any review, dissemination, distribution or copying of it is strictly prohibited. If you have received this in error, please notify us immediately via return email. Thank

you.\*\*\*\*\*  
\*\*\*\*\*



333 Bloor Street East  
Toronto, Ontario M4W 1G9  
Tel. (416) 935-7211  
Fax (416) 935-7719  
dhunt@rci.rogers.com

December 16, 2002

Vice-President  
Government & Intercarrier Relations

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, ON K1A 0H8

**EMAILED TO: la-al@justice.gc.ca**

Dear Mr. Paul Pierlot:

**Re: Comments – Lawful Access Consultation Document**

Rogers Wireless Inc. is pleased to file the attached comments in response to the public consultation initiated by The Department of Justice, Industry Canada and the Solicitor General Canada entitled '**Lawful Access – Consultation Document**'.

If there are any questions regarding these comments, please do not hesitate to contact the undersigned.

Sincerely,

A large rectangular area of the document has been redacted with a grey box, obscuring the signature and name of the undersigned.

s.19(1)

A handwritten signature in dark ink, appearing to be "J.P.", is written over the redacted signature area.

Attach.

**Department of Justice Canada  
Industry Canada  
Solicitor General Canada**

**LAWFUL ACCESS  
CONSULTATION DOCUMENT**

---

**COMMENTS OF  
ROGERS WIRELESS INC.**

---

**December 16, 2002**

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

### EXECUTIVE SUMMARY

1. Rogers Wireless Inc. ("RWI") is pleased to submit the following comments in response to the public consultation initiated by The Department of Justice, Industry Canada and the Solicitor General Canada (collectively "the Departments") entitled '**Lawful Access – Consultation Document**' ("the Consultation Paper").
2. In the Consultation Paper, the Departments have invited public comments regarding various proposals relating to a legal framework for lawful access.
3. RWI has also participated in the development of the comments that have been filed by the Canadian Wireless Telecommunications Association ("CWTA") and fully supports the CWTA's comments in their entirety.
4. RWI currently operates Canada's largest national commercial mobile communications services network, providing coverage to over 93% of the Canadian population. RWI's national network is comprised of fixed, mobile, circuit- and packet-based technologies, which employ a variety of technical standards. RWI believes that it is uniquely positioned to provide the Departments with constructive and relevant input regarding the Consultation Paper.
5. RWI is concerned that, absent the recommendations put forward by RWI in the following comments, a number of legislative proposals being considered by the Departments may curtail the quality, affordability and availability of wireless services in Canada, and may undermine the competitiveness and health of the wireless industry.
6. RWI also strongly recommends that the Departments provide an additional opportunity for stakeholders to provide comments once the proposed technical requirements are made available to stakeholders.
7. As set out in greater detail below, RWI strongly urges the Departments to ensure that the following principles and guidelines are incorporated in the new legal framework:

## **COMMENTS OF ROGERS WIRELESS INC.**

## **Lawful Access**

---

### **Principles**

- The new legislative framework will equitably balance the objective of maintaining lawful access capabilities with the objective of providing affordable and high quality telecommunications services in Canada and with the objective of enhancing the efficiency and competitiveness of the Canadian telecommunications market.
- The new legislative framework will recognize that the benefits associated with lawful access accrue to all Canadians. Lawful access costs will not be the responsibility of service providers.

### **Guidelines**

- Service providers will not be obligated to pay the costs of lawful access capabilities when the capabilities have not been incorporated into network hardware and software on the basis of industry standards and made available by technology vendors.
- Service providers will not be obligated to provide customer name and address information that they are not already collecting, validating and maintaining in the normal course of business.
- Service providers will not be obligated to preserve and retain data that they are not already collecting and maintaining in the normal course of business.
- Service providers will not be obligated to provide lawful access for network systems and data that they use in the provision of services, but which are owned and controlled by a third party.
- Service providers will be provided with the opportunity to request forbearance from any requirements that they cannot reasonably be expected to satisfy.

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

### BACKGROUND

8. Currently, wireless service providers ("WSPs") that are licensed to operate in the 1900 MHz Personal Communications Service ("PCS") band have, as a condition of their spectrum licence(s), an obligation to provide lawful access and interception capabilities that are consistent with the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications*. This obligation applies solely to circuit-switched voice telephony systems operating in the PCS band.
9. Licensees can request the Minister of Industry to forbear from enforcing certain of these requirements for a limited period.
10. It should also be noted that WSPs enter into business arrangements with law enforcement and security agencies to provide lawful access and interception capabilities for systems and frequency bands not covered by the condition of licence noted above.
11. WSPs already provide customer information to law enforcement and security agencies pursuant to a judicial warrant.
12. RWI understands that, in many respects, the requirements under discussion in the Consultation Paper go well beyond the existing requirements that apply to PCS licensees.

### DETAILED COMMENTS

#### **The Departments' Proposal**

13. RWI has reviewed the Consultation Paper and has also participated in face-to-face consultations with the Departments.
14. At the outset, RWI is concerned with the vagueness of the Departments' proposal. Despite the potentially far-reaching impact of the issues under consideration in the Consultation Paper, RWI notes that certain key elements of the proposal have not been defined.
15. Adding to this lack of clarity is the fact that detailed lawful access requirements and proposed regulations have not been provided to the stakeholders. Effectively, stakeholders are being asked to comment on a proposal that has not been adequately disclosed to them.
16. It is because of these uncertainties that RWI endorsed a letter that was sent by the CWTA to the Minister of Justice on November 1, 2002 requesting,

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

among other things, that draft legislation and regulations be provided for public comment.

17. RWI believes that the Departments are not adequately informed at present to define the new technical requirements, or to define deadlines by which service providers must be compliant with the new requirements. Nor will the Departments be adequately informed once the present consultation has been completed since, as noted already, details regarding the new requirements have not been provided in the Consultation Paper. Therefore, further consultation is an imperative that is urgently required.

18. RWI strongly believes that support for additional consultation is also found within the Consultation Paper itself.

19. For example, the Consultation Paper proposes that:

*Technical standards and details could be specified in the regulations.*

20. As noted already, the proposed detailed technical standards and regulations have not been provided by the Departments within the Consultation Paper. Nor have these details been provided by means of the face-to-face consultations that have conducted between the Departments and the stakeholders.

21. Elsewhere in the Consultation Paper it states that:

*Before recommending any regulation to Cabinet, the Minister of Industry and the Solicitor General would consult with appropriate persons representing the interests of those affected by the regulations.*

22. Clearly, the Departments are not in a position to recommend regulations containing detailed technical requirements to Cabinet, given that they have not consulted with stakeholders regarding such details. They have yet to confirm the reasonableness of the proposed requirements and, presently, cannot understand the impact of the new requirements on the stakeholders.

23. RWI strongly recommends that an additional consultation be undertaken between the Departments and the stakeholders once the proposed technical requirements are available for the consideration of the industry. Only then can the Departments and stakeholders participate in an informed discussion regarding the reasonableness of the proposed requirements and regarding the timing of the coming into force of the new requirements. Afterwards, the Departments will be equipped to recommend the proposed regulations to Cabinet.

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

24. In any event, RWI believes that technology incorporating the new requirements may not be available for a number of years. Technology vendors will only begin to incorporate the new requirements into their products after industry standards have been finalized. These industry standards will be driven primarily by the requirements of other jurisdictions, namely the United States and the European Union. Therefore, the timing associated with the availability of new products will not be determined by any timing that is imposed by the Departments. In light of these facts, there would appear to be no public benefit in proceeding with haste at the expense of an adequate consultation.

25. RWI appreciates the opportunity to provide the following comments regarding the general issues that are outlined in the Consultation Paper.

### Balancing Policy Objectives

26. RWI strongly believes that the new legislative framework should not assign a greater priority to the objective of maintaining lawful access capabilities than to the following objectives of Canadian telecommunications policy:

- *rendering reliable, affordable and high quality telecommunications services in Canada; and*
- *enhancing the efficiency and competitiveness of Canadian telecommunications.*

27. Lawful access and telecommunications policy objectives must be carefully balanced.

28. This is critical since, without the right balance, the proposals under consideration may well result in significant costs and potentially burdensome requirements being imposed on WSPs to the detriment of the Canadian wireless industry.

29. The imposition of significant costs on service providers would likely have the effect of driving the rates for wireless services upward, since service providers will have no alternative but to pass these costs onto their customers in the form of higher rates. This in turn may curtail the extent to which Canadians adopt wireless services. It should be noted that the Canadian wireless adoption rate (also known as 'penetration') is already among the lowest in the industrialized world.

30. Further, burdensome requirements and costs could stall, if not prevent, the provision of advanced communications services by service providers to their customers. This is of particular concern given that new and innovative services provided by WSPs play a crucial role in the Federal Government's *Innovation* strategy by enabling Canadians in all regions to be more efficient



## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

and productive, and by providing them with access to the information highway.

31. In some cases, the cost of incorporating lawful access capabilities may upset an otherwise favorable business case for a given service. It is also possible that, absent the proper balance, service providers will be prevented from providing some new and innovative services on the basis that, due to cost or technical constraints, the new services may not be able to satisfy all aspects of the required lawful access capability.
32. Similarly, service providers might be prevented from providing specific services, or from using certain distribution methods, if doing so will not result in the collection and validation of customer information that law enforcement and security agencies desire. This could make it more difficult for Canadians to purchase wireless services.
33. These potential results are not consistent with Canadian telecommunications policy and, therefore, they must be avoided.

### Costs and Funding

34. The Consultation Paper suggests that:

*lawful access is an essential tool in the prevention, investigation and prosecution of serious offences and the investigation of threats to the security of Canada.*

35. Given that the potential benefits arising from lawful access accrue to all Canadians, RWI strongly believes that the costs associated with lawful access should be born by all Canadians. The costs of lawful access should not be the responsibility of service providers.
36. That these costs should be born by the general public rather than service providers appears to have been recognized in other jurisdictions where a legal framework has been established for lawful access. For example, the legal frameworks established in the United States and United Kingdom provide direct or indirect funding for the cost of incorporating lawful access capabilities into network technology.
37. The Consultation Paper proposes the following regime governing costs:
  1. *Service providers would be responsible for the costs associated with providing the lawful access capability for new technologies and services, and*

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

2. *Service providers would be responsible for the costs associated with providing a lawful access capability when a significant upgrade is made to their systems or networks, however*
  3. *They would not be required to pay for necessary changes to their existing systems or networks.*
38. RWI notes that, in two of the three circumstances covered by the proposed regime, service providers would be responsible for the costs associated with a lawful access capability. In the remaining circumstance, service providers would not be responsible for the costs. It would appear that the Departments have proposed this cost regime based on the following assumptions.
39. First, the Departments have assumed that the cost of retroactively-fitting existing systems or networks to provide new lawful access capabilities will be substantial. In light of this fact, the Departments have proposed that service providers will not be responsible for such costs.
40. Based on its practical experience with retro-fitting existing equipment to provide new capabilities of any kind (not only lawful access capabilities), RWI concurs with the Departments' assumption. Generally speaking, costs associated with retro-fits are significant.
41. The Departments have also assumed that, in comparison to the cost of retro-fits, the cost of incorporating new capabilities into the design of a new system or network from the beginning are usually lower. The same assumption is made with respect to the cost of incorporating new capabilities into a "significantly upgraded" service.
42. Lastly, the Departments have assumed that the cost of incorporating new capabilities into the design of a new system or network, or into a "significantly upgraded" service, are not substantial and are insignificant. The Departments have proposed that service providers be responsible for these costs. It is with respect to this last assumption that RWI disagrees with the Departments.
43. It has been RWI's experience that, although the cost of incorporating capabilities into new systems and networks are generally lower than the cost of retro-fitting existing systems, they are by no means insignificant. RWI's experience has been that technology vendors apply significant explicit charges for many of the services and capabilities that they provide in conjunction with new systems and networks.
44. Even when services and capabilities are included in the standard package that is purchased by a service provider, significant activation charges must be paid to the vendor before a given service or capability can be activated. In the case of lawful access services and capabilities, the explicit charges that apply are in the order of millions of dollars.

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

45. RWI concedes that, in time, the cost of incorporating some services or capabilities into new systems or networks will become relatively insignificant and will no longer require the application of explicit charges. For example, several years ago, CCS7 signalling capabilities were made available by technology vendors only as a custom feature and only on the basis of an explicit charge. Over the course of several years, as technology and networks have evolved, vendors have elected to embed CCS7 signalling capabilities within their basic feature package, and they no longer apply an explicit charge for these capabilities. Presumably, the cost of providing these capabilities is no longer as significant as it once was and it is now implicit in the cost of the basic feature package.
46. In light of these facts, RWI strongly urges the Departments to revise the proposed regime such that service providers will only be responsible for the cost of providing lawful access capabilities in new systems or networks, or in significantly upgraded services, when the cost of doing so is no longer significant and is implicit in the cost of the basic feature package.
47. Otherwise, as long as the cost of providing lawful access for existing, significantly upgraded, or new services and networks is significant, and as long as the capabilities in question are only available upon payment of explicit charges, public funding should be provided.
48. With respect to costs associated with operational assistance that is provided to law enforcement and security agencies, RWI strongly recommends that the new framework explicitly recognize that fees imposed for the recovery of these costs are valid. Some agencies, including federal agencies, have acknowledged the reasonableness of these fees and have been paying them for a number of years. These costs should not be the responsibility of service providers, but should be reflected in the agencies' cost of undertaking investigations.

### Definition of Key Terms

49. The Consultation Paper proposes that:

*All service providers would be required to provide, at a minimum, a basic intercept capability before providing new services or a significantly upgraded service to the public.*

50. The Consultation Paper does not explain what a "basic intercept capability" comprises. Service providers are left to speculate what this capability might entail. In any event, the inclusion of the words "at a minimum" suggests that something above and beyond a "basic intercept capability" may be required.

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

- 
51. Without a precise definition of the capability in question, service providers cannot adequately understand the potential impact and cost of this proposal.
52. RWI also notes that the circumstances in which service providers will be required to cover their cost of compliance are not clear. While *"new technologies and services"* is relatively clear, the reference to a *"significant upgrade"* is hazy at best and no clarification of this term is supplied in the Consultation Paper.
53. Since the Departments have proposed that service providers will be obligated to provide a *"basic intercept capability"* before providing a *"significantly upgraded service to the public"*, the definition of a *"significant upgrade"* will have important implications for service providers.
54. RWI notes that lawful access capabilities are primarily provisioned in the hardware and software of a service provider's core network. In some cases, wholesale and extensive modifications to the core network may provide an opportunity for service providers and network vendors to implement additional lawful access capabilities.
55. On the other hand, relatively minor and incremental enhancements to certain aspects of the network, such as the addition of a network element or service node, the expansion of geographic coverage, and the installation of interconnection facilities, do not represent opportunities to enhance or increase lawful access capabilities. The same is true for routine operational modifications such as increasing the traffic handling capacity of a switch, or the re-tuning of wireless base stations. Service providers and vendors cannot reasonably be expected to implement additional lawful access capabilities in these instances.
56. It is important to note that, even in cases where extensive modifications are made to the core network, the implementation of additional lawful access capabilities can only be reasonably expected if technology vendors have incorporated the capabilities into core network technology. Equally important is that vendors have incorporated the capabilities on the basis of industry standards.
57. Solutions that are based on industry standards are to be preferred over those that are based on proprietary approaches for a number of reasons. Technology solutions based on industry standards are more likely to result in larger economies of scale, better availability of products, a migration path to future enhancements, and greater potential for interoperability and compatibility within and between networks.
58. In the context of lawful access, solutions based on industry standards will, for example, result in more standardized technical interfaces and output formats
-

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

provided to law enforcement and security agencies, regardless of the service, the service provider, or the technology vendor in question. This will translate into more simplified processes and lower costs for law enforcement and security agencies.

59. RWI is opposed to the notion that proprietary or uniquely Canadian solutions for lawful access will be imposed on service providers.

60. In light of the above, RWI recommends that a "*significant upgrade*" be defined within the new legislative framework as the replacement of the entire hardware and software platform utilized by the service provider's core network.

61. Where technology vendors have not incorporated the required lawful access capabilities in the core network on the basis of industry standards, service providers must not be required to pay the cost of these capabilities, and must not be prevented from implementing an upgrade, or from offering new services.

62. RWI further recommends that "*core network*" be defined as the physical entities that provide support for the network features and telecommunication services. The support provided includes functionality such as the management of user location information, control of network features and services, the transfer (switching and transmission) mechanisms for signalling and for user generated information.

63. RWI notes that its proposed definition of a "*core network*" is derived from, and consistent with, current industry standards (specifically, 3GPP TS 23.101 V4.0.0).

64. RWI believes that the adoption of these definitions into the framework will ensure that service providers will be expected to implement additional capabilities only when they have a reasonable opportunity to do so and only when the capabilities are available on the basis of industry standards.

65. RWI also believes that service providers must not be responsible for lawful access with respect to network systems that are used in the provision of services, but which are owned and controlled by a third party. This is important given that, for example, network systems associated with certain services provided by WSPs are, in many cases, under the control of third parties such as application service providers and technology vendors.

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

### New Services

66. RWI believes that the Departments' proposal may have a "freezing" effect on new and innovative services, particularly those services that would be introduced in the months following the imposition of the new requirements.

67. RWI notes that a significant amount of time is required before technology vendors can incorporate new requirements into the design cycle of their products. The development of newer versions or generations of telecommunications products is often a matter of years. RWI believes that the law enforcement and security agencies are well aware of this fact as a result of their relationships with technology vendors and with service providers.

68. Technology vendors will have no clear understanding of the new requirements until these requirements are made available. Once they have been made available, the new requirements can be incorporated into the vendors' product design cycle. After an appropriate amount of time has elapsed, products that incorporate the new requirements will be made available to service providers.

69. In view of these realities, RWI believes that the new legal framework should incorporate a "grace period" that would apply immediately following the coming into effect of the new requirements and that would extend for a period of no less than 18 months. During this period, service providers will be permitted to introduce services that may or may not be capable of satisfying all of the new requirements. After this period, vendors will be considered to have been given adequate time to develop and incorporate the new requirements into their products, and to make these products available to service providers.

70. In the absence of a "grace period", service providers will be prevented from offering new services for a significant amount of time following the introduction of the new requirements, since vendors will not have had ample opportunity to incorporate the new requirements into their products. This "freezing" effect could have a devastating impact on service providers and would deprive their customers of new and innovative services. These results would not be consistent with the Canadian telecommunications policy objectives noted above.

### Forbearance

71. RWI fully supports the proposal that the new framework provide a system of forbearance and agrees with the Departments that a system of forbearance would provide a necessary degree of flexibility in the new framework. RWI

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

believes that a system of forbearance, similar to that which is already used for PCS licensees, should be included in the new framework such that service providers can seek forbearance, as required, beyond the 18 month "grace period" that RWI has proposed.

72. RWI believes that any compliance mechanism that may be adopted in the new framework must incorporate a means by which service providers that have been found to be non-compliant will be given a reasonable amount of time to become fully compliant. As noted above, additional lawful access capabilities can only be provided once technology vendors have incorporated such capabilities into the design of their products.
73. Therefore, RWI recommends that service providers be given a period of 18 months to come into compliance. Where the required lawful access capabilities are already available in a service provider's technology, this duration could be reduced to 6 months.

### Subscriber Information

74. The Consultation Paper asks whether a legal requirement should be created so that service providers can be required to provide law enforcement and security agencies with customer information such as name, billing address, phone number, name of service provider and email address. The Consultation Paper also points out that such information is already routinely provided under certain circumstances.
75. In response, RWI is not opposed to making information available to law enforcement and security agencies, to the extent that the information is available and pursuant to a judicial warrant.
76. Generally, WSPs collect, validate and maintain customer information to the extent that such information is necessary to successfully provide service and to collect payment. For postpaid services, WSPs will typically undertake a credit check to determine a prospective customer's ability to make monthly payments for the services provided. However, this process is geared to validating credit worthiness, not to validating the customer's name and address. WSPs do not undertake exhaustive validation of the information that is provided by customers and, therefore, WSPs do not warrant that such information is valid or correct, or that it would satisfy the requirements of law enforcement and security agencies. Further, WSPs are almost entirely reliant on customer-initiated notification with respect to address changes.
77. Significant service, business and cost issues could arise if WSPs are required to collect, validate and maintain accurate customer information for the purposes of lawful access. First, any such requirement would likely obligate WSPs to insist that customers present a minimum degree of official



## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

identification at the point of purchase. This would also require that WSPs, and the variety of independent distribution agents and outlets they rely on, would be capable of validating such identification.

78. An overwhelming issue would arise with respect to on-line purchases of wireless services since, for these purchases, the entire transaction is conducted over the Internet, not in person. Similarly, customers who opt for on-line billing will be billed on-line and will not have a monthly invoice sent to a physical address. If they choose to move, the carrier will have no means of knowing, apart from the customer taking the initiative to update this information by accessing their on-line account.

79. In the case of purchasing or billing, on-line transactions do not lend themselves to the presentation and validation of the customer's identification. WSPs, and countless other businesses in Canada and abroad, have already made significant investments in on-line purchasing, billing and customer relations capabilities and they rely on this channel as a useful and cost-effective means by which to acquire, bill and interface with their customers.

80. Another problem would be created with respect to prepaid wireless services provided by WSPs since valid customer information is not required to provide prepaid services. Given that a credit check is not required, and that the customer will never receive a monthly bill, there is no need for the WSP to request the customer's name or address. The entire transaction of activating the customer's account can be conducted over the phone and absent any identification. Although WSPs are increasingly requesting customer name and address information for business purposes, this information is not validated, nor do WSPs deny service if the customer does not provide the information.

81. In light of the above, RWI is opposed to the imposition of any new requirements that will significantly impact existing services, distribution channels and business processes, all of which have been developed by WSPs for business purposes such as the provision of services and the collection of revenues.

82. Similarly, RWI strongly believes that WSPs must not be required to eliminate certain distribution channels or services if specific customer information cannot be obtained by means of these channels, or services.

83. RWI is also opposed to the proposal that an industry-wide database, or registry, containing customer and/or service provider information be created for lawful access purposes. As noted above, customer information is already provided to law enforcement and security agencies pursuant to a judicial warrant. RWI also notes that service provider information is accessible by



## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

means of publicly available data. RWI encourages the Departments to consider the comments provided by the CWTA in this regard.

### Preservation and Retention of Data

84. The Consultation Paper proposes that the new legal framework incorporate the concept of a *"data-preservation"* order. RWI understands that these temporary orders would only apply in special circumstances in order to preserve data until law enforcement agencies can obtain a judicial warrant to obtain the data. RWI also understands that these orders would only apply to *"existing data that is specific to a transaction or client"*.
85. In response, RWI strongly believes that the new framework should only obligate service providers to preserve data that is already collected and maintained in the normal course of business, and only for a specific instant in time. Service providers must not be obligated to preserve data that they have no capability to access or to preserve.
86. Similarly, service providers must not be under any obligation with respect to data that they use in the provision of services, but which is owned and controlled by a third party. This is important given that, for example, content associated with certain services provided by WSPs is, in many cases, under the control of third parties such as application service providers and technology vendors.
87. Further, RWI believes that the framework should stipulate that service providers served with a data-preservation order will be required to preserve the data in question for a period not exceeding 4 days when the necessary judicial warrant is provided by the Canadian judicial system. In circumstances where warrants are required from judicial systems in other jurisdictions, this period could be extended as required, but must not exceed 90 days.
88. The Consultation Paper makes reference to *"data-retention"* which is defined as *"a general requirement that could compel service providers to collect and retain a range of data concerning all of its customers"*.
89. RWI is pleased that the Departments are not contemplating a data-retention requirement within the new legal framework. RWI would be strongly opposed to any requirement for data-retention. A sweeping requirement such as this would likely have a significant negative impact on the operations of service providers and would contribute to substantial storage costs.

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

### Virus Dissemination

90. RWI strongly encourages the Departments to ensure that the new framework make it clear that service providers will not be held liable from a criminal or civil perspective for any virus that has been introduced to their systems by their customers, or by customers of other service providers.

91. RWI is not opposed to the notion that service providers will be expected by means of a judicial warrant to give assistance to law enforcement and security agencies in eliminating any virus that has been introduced to the service providers' networks and which is being used for criminal purposes.

### CONCLUSION

92. For the reasons outlined above, RWI also strongly recommends that the Departments provide an additional opportunity for stakeholders to provide comments once the proposed technical requirements are made available to stakeholders.

93. RWI strongly urges the Departments to ensure that the new legal framework for lawful access will reflect the following:

- The new legislative framework will equitably balance the objective of maintaining lawful access capabilities with the objective of providing affordable and high quality telecommunications services in Canada and with the objective of enhancing the efficiency and competitiveness of the Canadian telecommunications market.
- The new legislative framework will recognize that the benefits associated with lawful access accrue to all Canadians. Lawful access costs will not be the responsibility of service providers.
- Service providers will not be obligated to pay the costs of lawful access capabilities when the capabilities have not been incorporated into network hardware and software on the basis of industry standards and made available by technology vendors.
- Service providers will not be obligated to provide customer name and address information that they are not already collecting, validating and maintaining in the normal course of business.
- Service providers will not be obligated to preserve and retain data that they are not already collecting and maintaining in the normal course of business.

## COMMENTS OF ROGERS WIRELESS INC.

## Lawful Access

---

- Service providers will not be obligated to provide lawful access for network systems and data that they use in the provision of services, but which are owned and controlled by a third party.
- Service providers will be provided with the opportunity to request forbearance from any requirements that they cannot reasonably be expected to satisfy.

94. Finally, RWI appreciates the opportunity to provide its comments regarding the Consultation Paper.

\*\*\* End of Document \*\*\*

Pierlot, Paul

From: [REDACTED]@gov.ab.ca] s.19(1)  
Sent: 2002 Dec 16 4:33 PM  
To: 'la-al@justice.gc.ca'  
Cc: 'Angers, Lucie'  
Subject: Response of Alberta Justice (Criminal Division) -Lawful Access Co nsultation

Importance: High



Lawful Access  
Consultation Res...

Lucie, I apologize for sending this message directly to you, but I am having some difficulty sending the message to the address listed in the consultation document.

I trust that all is well, and hope that you will be able to take some time off over the holidays. Best Wishes,  
[REDACTED]

I have been asked to send the following response on behalf of [REDACTED] Assistant Deputy Minister (Criminal Justice). A signed original will follow.

Thank you for providing this opportunity to provide feedback on this important undertaking.

<<Lawful Access Consultation Response.doc>>

This communication is intended for the use of the recipient to which it is addressed, and may contain confidential, personal and/or privileged information. Please contact the Justice/Solicitor General HelpDesk (Help.Desk@gov.ab.ca) @ (780) 415-2998 immediately if you are not the intended recipient of this communication, and do not copy, distribute, or take action relying on it. Any communication received in error or subsequent reply, should be deleted or destroyed.

JUSTICE

Office of the Assistant Deputy  
Minister (Criminal Justice)

9833 - 109 Street  
Edmonton, AB  
Canada, T5K 2E8

Telephone 780/427-5046  
Fax 780/422-9639

December 16, 2002

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, Ontario K1A 0H8

Dear Sir or Madam:

**RE: Lawful Access Consultation**

In August of 2002, the Government of Canada announced a formal consultation process in relation to the issues surrounding lawful access to all forms of electronic communication and data. Alberta Justice welcomes the opportunity to respond to this consultation, and to continued participation in the detailed development of these proposals within the Federal / Provincial / Territorial working group on Cyber-crime. We recognize that the responses of other government departments and agencies emphasize issues of particular concern to their respective mandates.

s.13(1)(c)

s.14

s.21(1)(a)

**Background**

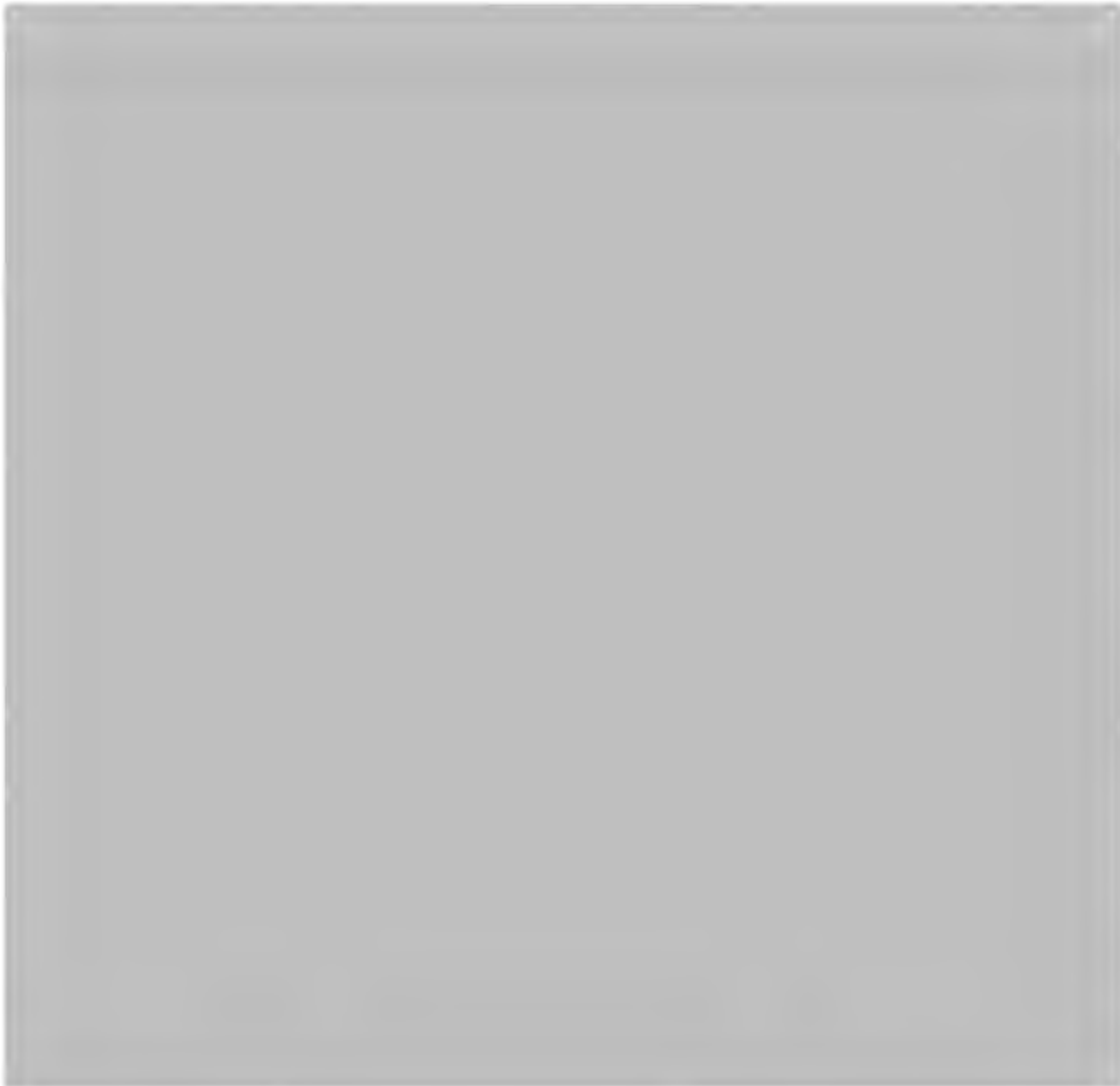
The rapid development and use of highly sophisticated means of electronic communication is becoming a common occurrence in all aspects of society. While this has led to several benefits to society at large, there can be no doubt that it has also given rise to new challenges. Foremost among these is the ability of law enforcement to retain the technical and legal tools needed to track, seize, and intercept such communications with appropriate judicial authorization.

The use of sophisticated new communication tools in all facets of criminal activity is increasing. This is particularly true in the areas of serious, violent and organized crime, and child pornography.

**Proposed Approach**

s.13(1)(c)

s.21(1)(a)



We appreciate the opportunity to express our strong concern regarding this issue, and look forward to working towards a detailed implementation of these principles through established Federal /Provincial / Territorial working groups.

Yours truly,

  
Assistant Deputy Minister

s.19(1)

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 16 4:55 PM  
To: la-al@justice.gc.ca; consultations@canada.justice.gc.ca; [REDACTED]  
Subject: Response to Lawful Access Consultation

Hello,

I have recently reviewed the Lawful Access consultation documents as posted on the Department of Justice website. I have attached a series of comments on the proposed legislative options.

I am an Information Security professional with seven years of industry tenure, so I speak here from a position of some expertise and knowledge on such matters.

#### 1) Intercept Capability

No legislation should be introduced that enforces a formal system of data interception points throughout the entirety of the Canadian electronic infrastructure. Such a system is vulnerable to abuse.

##### 1.1) Requirement to provide interception capability

I am familiar with the technical architecture of the Canadian Internet backbone. Special requirements to provide intercept capability are not even technically necessary in the majority of cases. Intercept equipment often uses interfaces that are compatible with hardware present in most machine rooms. Network equipment in many cases offers diagnostic capability which will facilitate lawful interception.

Additional requirements to provide explicit capability to intercept Internet traffic therefore do not appear to be necessary.

The following questions remain, however, even for current intercept equipment:

- a) Does intercept equipment remain connected indefinitely, and if so, through what means do providers gain assurance that data is not being intercepted on an ongoing basis?
- b) What is the means in place to dissuade constant interception, once the technical deterrent of engineering a specific intercept point for each investigation has been removed?

##### 1.2) Costs to provide capability

There should be no cost to any telecommunications firm to provide a service which permits easy interception of data from privately-owned networks.

All costs must be borne entirely by law enforcement agencies and/or the Government of Canada if such a program is eventually devised.

#### 2) Production, Anticipatory, and General Orders

Production orders are unnecessary given the ability of law enforcement agencies to obtain information via existing means.

I do not agree with the rationale for issuance of anticipatory orders.

"should there be a specific power, parallel to that provided for

in the Criminal Code dial number recorders, to allow law enforcement and national security agencies to obtain traffic data?"

Absolutely not. Why would intelligence agencies be granted access to the data of Canadians based on a model created for the investigation of criminal activities?

In addition, "traffic data" may constitute the actual content of a given network communication. A dial number recorder is not a wiretap, but a "traffic data" intercept can easily play that role. It would therefore be inaccurate to directly equate an intercept device capable of obtaining data content from network "traffic" and a dial number recorder.

This power should not be enacted.

"should there be a specific production order in relation to customer name and address and service provider information?"

No. Warrants and court orders should be issued for this purpose. If law enforcement agents cannot convince a court to issue such, this is not a rationale by which to create new powers. I remain concerned that a production order could be obtained where insufficient cause exists to believe that a specific criminal act has been committed.

Personal information must be protected unless a specific criminal act is being investigated. Any request by law enforcement is not itself a rationale by which to provide personal information unless that request is a component of a court proceeding or investigation likely to result in such a proceeding.

### 3) Data-preservation orders

No Data-preservation order should be issued without a warrant. The model presented suggests that such an order will be issued before a warrant is obtained. I am concerned, therefore, that such an order could be procured without reasonable cause.

Regarding customer data collection, no telecommunications firm should be required, as a daily business practice, to compile what is essentially intelligence information on their user base (especially where no crime is suspected and no specific individual is targeted for investigation).

### 4) Virus dissemination

The wording of this section, and the focus on "virus" dissemination, is profoundly limited in both applicability and utility due to the following:

- 1) A significant number of mobile code threats are not "viruses"
- 2) A significant threat is posed by code that is not mobile

In general I have found most attempts to codify "cybercrime" laws have been disproportionately centred around "virus" programs. This has always struck me as misguided. I remain concerned that such a focus speaks to an insufficient level of consultation with those within the information security field.

The problems with the limitations of this section are as follows:

#### a) Virus programs are not the only serious mobile code threat

There are many mobile, automated programs that exist which cannot be described as a "virus" in a strict sense. That this section is



titled "Virus Dissemination" concerns me, because it implies (to me) the possibility that other threats have not been fully explored and understood.

b) Mobile code is not the only serious threat

Some of the most serious security exposures I have dealt with over the last seven years have had nothing to do with mobile code or a "virus" program. This reality, however, is entirely absent from the discussion presented in the lawful access documentation, raising the concern that insufficient consultation with the security community has been conducted within Canada prior to creation of this proposal.

Two examples I would like to specifically mention for your review include the suite of SNMP vulnerabilities discovered in early 2002 and the distributed denial of service attacks launched in February 2000. Neither of these incidents constituted "Virus Dissemination", yet both rocked the information security community and IT field.

c) Remedies which target virus authors/users alone necessarily target a very limited proportion of the intruder community

While it is true that some skilled individuals have created complex and potent mobile code, it is also true that amateurs can release a prefabricated virus program. It is again true that highly talented, capable members of the intruder community will never, in any of the deeds they commit, make use of a "virus" program or mobile code. The disproportionate focus on "Virus Dissemination" fails to address an attacker of this calibre.

The proposal assigns a primacy to packaged virus toolkit software that threatens to eclipse the threat posed by more experienced, gifted attackers. I submit that our priorities must be more nuanced.

d) Some attacks require no specialized tools

The "Virus Dissemination" provision will provide no assistance when prosecuting so-called "insider" attacks where no special software is required to successfully cause expensive levels of business impact, despite the fact that these attacks are widely considered to be those most likely to strike a given organization.

My specific responses to statements and legislative options are as follows:

"Under the current provisions of the Criminal Code, only the effects of spreading a computer virus, or an attempt to do so, are criminal acts."

The Criminal Code should NOT be modified from this wording. It is my opinion as a security professional that changing the wording of the Code will in this instance not result in a reduction of risk, but instead only jeopardize valuable, legitimate security research.

"The Council of Europe Convention on Cyber-Crime requires signatory states to criminalize the creation, sale and possession without right of devices (e.g., computer programs) that are designed or primarily adapted for the purpose of committing offences specified in the Convention, whether or not the virus has been deployed or has caused any form of mischief."

There are many serious problems inherent with this rationale. It is my opinion that the Council of Europe was in error when this language was included within the Cyber-Crime Convention. I do not believe Canada should ratify any agreement that criminalizes software programs, primarily because I do not believe it will meaningfully reduce risk.

The issues I have with the rationale presented are as follows:

a) Every information security professional involved with assessments and testing possesses software applications which fit the description of a criminal device above. Every security researcher who develops a proof-of-concept computer program to demonstrate security exposures would be similarly guilty of a criminal offense.

In many cases, these software applications are the EXACT applications used by criminals. There will be no means of differentiating between a "legitimate" tool and a "criminal" tool be means of examining tools or computer programs themselves. Some are even written by intruders.

I do not want the onus placed upon myself and other members of the security community to demonstrate our lack of intent or presence of legitimacy when we hold such tools. I am seriously concerned that information security research in Canada will be subject to a deeply chilling effect if the Code is amended to criminalize any type of computer software.

b) It should be noted that there have been recent examples of court opinion in the United States which hold that the act of writing a piece of computer software is a protected act of free expression. The rationale suggested by the Council of Europe may be subject to Charter challenge if Canadians within the research and security community maintain that protections must be extended to the act of writing a computer program.

c) Creating new criminal acts does not arrest and convict people, law enforcement does. Both federal and provincial law enforcement groups lack adequate resources for investigating and prosecuting computer crime. Until this situation is corrected, criminalizing entire genres of software applications will do nothing to aid in the actual prosecution of criminal acts or deter those who would commit them.

In short, it is my professional opinion that:

- a) Council of Europe criminalization of software is wrong-headed
- b) Criminalization will not address many serious security threats
- c) Criminalization will seriously impact the security community
- d) Criminalization will chill legitimate and important research
- e) Police resources are insufficient to enforce even existing laws
- f) Criminalization will not reduce the threat to Canadian systems

Do not alter the Criminal Code in this fashion. Do not ratify this convention if it requires such Code alterations. Please consult members of the information security community directly if further discussion of software criminalization is required.

#### 5) Interception of e-mail

There should be no differentiation between the postal mail system in this country and the use of e-mail to issue communications. At every step where postal mail would be considered a private communication, an e-mail message should also be considered a private communication.

Any specific proposal for the interception of e-mail must make very clear reference to the stages of the e-mail delivery process to make certain that the essence of private communication protection has been properly upheld.

#### 6) Service Provider Information

"what type of mechanism, if any, should be put in place to provide

law enforcement and national security agencies with up-to-date and accurate CNA and LSPID information while respecting the privacy of Canadians?"

Personal information which belongs to Canadians should not be provided to agencies when there is no reasonable likelihood of a legal proceeding. CNA, like any information which links a name to a number and physical location, is protected personal information.

"should an obligation to collect such CNA information be imposed even if the service provider does not collect this information for its own purposes? In other words, should a provider be compelled by law to collect CNA information?"

No. Companies should not be forced to request personal information they do not require for business purposes simply to provide it to RCMP and CSIS. The Government of Canada should in fact attempt to better protect Canadians from unnecessary requests for personal information.

The Government of Canada must cover all costs associated with a new CNA collection effort.

No police or security agency should operate CNA databases directly.

Thank you for your consideration of these responses. It is my sincere hope that the Government of Canada will carefully weigh any perceived benefit of these proposals with the potential for serious impact not only to the integrity of the information security industry, but also to the vital civil liberties of all Canadians.

I would be pleased to provide additional comment on request.

Yours truly,

s.19(1)

Toronto, Ontario

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 16 4:58 PM  
To: la-al@justice.gc.ca  
Cc: [REDACTED]  
Subject: Lawful Access Consultation: EFC and EFF

Lawful Access Consultation,  
Criminal Policy Section  
5th Floor,  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8

December 16, 2002

**RE: Request for Comments on "Lawful Access – Consultation Document "**

Electronic Frontier Canada (EFC) and the Electronic Frontier Foundation (EFF) appreciate the opportunity to submit comments on "Lawful Access – Consultation Document."

Attached please find the submission of EFC and EFF. This document is a result of efforts

By:

[REDACTED]  
Dept. of Computer Science  
McMaster University  
Hamilton, Ontario  
[REDACTED]

[REDACTED]  
Senior Staff Attorney  
+1 415 436-9333 x [REDACTED] (voice)  
+1 415 436-9993 (fax)  
[REDACTED]

[REDACTED]  
Dept. of Computer Science  
University of Waterloo  
Waterloo, Ontario  
[REDACTED]

Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, California 94110  
U.S.A.

[REDACTED]  
Dept. of Computer Science  
University of British Columbia  
Vancouver, British Columbia  
[REDACTED]

Electronic Frontier Canada  
20 Richmond Avenue  
Kitchener, Ontario  
N2G 1Y9

Sincerely,

## Comments of Electronic Frontier Canada and Electronic Frontier Foundation

Lawful Access Consultation,  
Criminal Policy Section  
5<sup>th</sup> Floor,  
284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8

December 17, 2002

RE: Request for Comments on Lawful Access – Consultation Document

Electronic Frontier Canada (EFC) and the Electronic Frontier Foundation (EFF) appreciate the opportunity to submit comments on "Lawful Access – Consultation Document." ("Proposal")

EFC's mandate is to conduct research into issues and promote public awareness in Canada regarding the application of the *Charter of Rights and Freedoms* to new computer, communication, and information technologies, such as the Internet. Its aim is protect freedom of expression and the right to privacy in cyberspace.

EFF is a non-profit, member-supported civil liberties organization working to protect rights in the digital world. With almost 8,000 active members worldwide, EFF actively encourages and challenges industry, government and the courts to support free expression, privacy, and openness in the information society. Founded in 1990, EFF is based in San Francisco and maintains one of the most-linked-to Web sites <<http://www.eff.org>> in the world.

### 1. Introduction

EFC and EFF oppose the Proposal as a vague and unjustified plan for intrusive covert surveillance of private communications that clearly threatens the fundamental values and fabric of Canadian society.

First, the Proposal radically expands surveillance powers over private communications, including Internet communications. The Internet is not merely a one-to-one medium of communication: it is a valuable yet inexpensive publication medium as well as a virtual assembly hall for political, religious and cultural association. As such, the Proposal threatens not only Canadians' right of privacy protected by s. 8 of the Charter but also the fundamental freedoms of expression and association protected by s. 2 and the right to liberty protected by s. 7.

Second, we seriously question the Proposal's general approach to communications privacy, which essentially contemplates making fine distinctions among telecommunications and data associated with telecommunications according to the mechanics of their transmission or use. From the individual's perspective, communications are communications, whether telephone conversations or e-mail. Why should the mere fact that Internet communications leave more detailed traces entail less privacy vis-a-vis the government in those communications? Why should individuals even need to think about whether their communications and associated data are more or less protected according to technical details about how they are stored, processed or transmitted?

Third, the Proposal cannot be evaluated in isolation; it must be viewed in light of other proposed erosions of privacy and freedom. For instance, it makes no sense to contemplate a

centralized national database of Internet subscribers without also considering the plan of the Canada Customs and Revenue Agency (CCRA) to establish a database on the foreign travel activities of Canadians. The experience of "function creep" teaches that "Big Brother" need not be built in a day.<sup>1</sup>

Fourth, we reject the Proposal's implicit assumption that Canada's participation in international instruments like the *Council of Europe Convention on Cybercrime* ("Convention")<sup>2</sup> can justify the Proposal. Insofar as Canada has not yet ratified the *Convention*, the Proposal is clearly premature. Significant public debate is necessary before Canada even ratifies the *Convention*. Moreover, Canada should not violate the rights of Canadians simply because other nations place less value on individual privacy. As we note below, s. 8 is more protective of privacy than the American Fourth Amendment.

Finally, we reject the Proposal's simplistic statement that law enforcement and national security agencies need to "maintain lawful access capabilities" in the face of technological developments. Not only would the Proposal increase such capabilities beyond their present scope,<sup>3</sup> s. 1 of the Charter requires that restrictions on rights must be "demonstrably justified" and consistent with "a free and democratic society." No such need been empirically demonstrated.

Equally important, it is illogical to use this supposed hindrance to law enforcement for one particular area to justify invading fundamental rights while ignoring the many technological developments that have helped law enforcement, such as advances in surveillance and forensic technology. An intellectually honest approach would frankly admit that computers have aided law enforcement activity in many ways and exposed more of individuals' daily transactions to monitoring, collection, and "data-mining." Indeed, the very notion of "maintain[ing] . . . capabilities" implicitly assumes that the present level of telecommunications privacy is socially desirable — a dubious assumption. Today, few electronic communications are encrypted; they would be more private if encryption were widely used. Using today's online world as a baseline essentially "freezes" privacy at its current level.

We therefore urge that the Proposal be rejected.

## 2. Background

Privacy is a value of fundamental importance in Canadian society. The Supreme Court has made clear that the Charter's function "is to provide . . . for the unremitting protection of individual rights and liberties,"<sup>4</sup> and that the purpose of the right "to be secure against

---

<sup>1</sup>The classic example is the American Social Security Number (SSN), which was originally instituted in 1934 as a way of indexing records for citizens qualified to receive benefits. At the time, politicians specifically commented that SSNs would not be used to implement a national ID system. Today, SSNs have expanded far beyond their original purpose and have essentially become a national ID number. R. Brian Black, *Legislating U.S. Data Privacy in the Context of National Identification Numbers: Models From South Africa and the United Kingdom*, 34 CORNELL INT'L L.J. 397, 411 (2001); see Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 499 & n. 98 (1999).

<sup>2</sup>Budapest, 23.XI.2001.

<sup>3</sup>See discussion at 3c - 6.

<sup>4</sup>*Hunter v. Southam, Inc.*, [1984] 2 S.C.R. 145, 155 [hereinafter *Hunter*].

unreasonable search or seizure" under s.8 "is . . . to protect individuals from unjustified state intrusions upon their privacy."<sup>5</sup> Moreover,

"that right, like other Charter rights, must be interpreted in a broad and liberal manner so as to secure the citizen's right to a reasonable expectation against governmental encroachments. Its spirit must not be constrained by narrow legalistic classifications based on notions of property and the like which served to protect this fundamental human value in earlier times."<sup>6</sup>

The Supreme Court has distinguished three types of privacy: territorial or spatial, personal, and informational.<sup>7</sup> The Proposal poses a great threat to the right to informational privacy, which "derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit."<sup>8</sup> In modern society especially, "retention of information about oneself is extremely important. We may . . . wish or be compelled to reveal such information, but situations abound where the reasonable expectation of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected."<sup>9</sup>

The protection of privacy against state intrusion has been of particular concern to the courts in assessing the validity of surveillance measures, due to the inequality of power in the relationship between individuals and the state, and the resultant vulnerability of individuals to state abuses of power. In *R. v. Duarte*,<sup>10</sup> the Supreme Court emphasized this distinction in finding unauthorized audiovisual surveillance to be unconstitutional:

"[T]he regulation of electronic surveillance protects us from a risk of a different order, i.e., not the risk that someone will repeat our words but the much more insidious danger inherent in allowing the state, in its unfettered discretion, to record and transmit our words.

The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning."<sup>11</sup>

---

<sup>5</sup>*Hunter* at 160.

<sup>6</sup>*R. v. Dymnt*, [1988] 2 S.C.R. 417, 426-427 [hereinafter *Dymnt*]. *Dymnt* suggests that individual privacy may also be protected as "liberty" under s. 7 of the Charter.

<sup>7</sup>*Dymnt*, at 428.

<sup>8</sup>*Dymnt*, at 429 (citation omitted).

<sup>9</sup>*Dymnt*, at 429-430.

<sup>10</sup>[1990] 1 S.C.R. 30.

<sup>11</sup>*Id.*, at paras. 21-22.

Another rationale offered for the Proposal is that other nations have updated their legislation, and changes in Canadian legislation are required for Canada to remain an "effective partner internationally."<sup>12</sup> Inasmuch as Canada has not yet ratified the *Convention*, this rationale is unconvincing; indeed, if ratification would result in Canada's being required to adopt the Proposal, then ratification is a bad idea. For instance, s. 8 of the Charter is more protective of privacy than the Fourth Amendment of the U.S. Constitution; in determining whether personal information is "private," American law focuses almost exclusively on whether the information is confidential, while Canadian law also looks at how a police practice would affect the freedom and dignity of the individual in a democratic society.<sup>13</sup>

Moreover, this rationale tells a very small part of the story. Attempts at passing such legislation have been fraught with problems in many nations (particularly in other Commonwealth nations), due to strong objections by a variety of parties, such as industry groups, academics, the media and civil liberties organizations. For example, in Australia, the *Telecommunications Interception Legislation Amendment Bill 2002*, which would have allowed interception of communications delayed or stored in transit without a warrant, was rejected by the Senate.<sup>14</sup> In South Africa, the *Interception and Monitoring Bill*, which mandated interception capability and permitted access to traffic data without a warrant, was dropped after the expression of significant opposition.<sup>15</sup> In the United Kingdom, there was positively an uproar amongst the media,<sup>16</sup> legal academics<sup>17</sup> and civil liberties organizations<sup>18</sup> over the *Regulation of*

<sup>12</sup> Department of Justice Canada, *Lawful Access - Consultation Document*, (Ottawa: Department of Justice, August 25, 2002) at 7.

<sup>13</sup> As one Canadian law professor has explained, Canada takes a normative approach to privacy. Jerome Atrens, *A Comparison of Canadian and American Constitutional Law Relating To Search and Seizure*, 1 SW. J.L. & TRADE AM. 29, 35 (1994). For instance, under U.S. law, there is no "search" under the Fourth Amendment when an undercover police agent converses with an accused and at the same time surreptitiously transmits the conversation to police officers who were transcribing the conversation. *United States v. White*, 401 U.S. 745, 751 (1971); id. at 752 ("Inescapably, one contemplating illegal activities must realize that his companions may be reporting to the police."). Under Canadian law, such "participant surveillance" is subject to s. 8. *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 11.

Another example is the treatment of electronic tracking devices. Under U.S. law, police may plant a radio transmitter beeper in a car without a warrant because a person's movements on public thoroughfares are not private within the meaning of the Fourth Amendment. *United States v. Knotts*, 460 U.S. 276 (1983). By contrast, in Canada such tracking is a search subject to s. 8 of the Charter. *R. v. Wise*, [1992] 1 S.C.R. 527.

<sup>14</sup> Privacy International, *Phone Tapping and Encryption News*, <<http://www.privacyinternational.org/issues/tapping/>> (date accessed: August 14, 2002).

<sup>15</sup> *Ibid.*

<sup>16</sup> See for example, "British Liberty, RIP" *The Guardian*, June 11, 2002, <<http://www.guardian.co.uk/Archive/Article/0,4273,4431010,00.html>> (date accessed: August 14, 2002).

<sup>17</sup> See, e.g., Y. Akdeniz, N. Taylor, and C. Walker, *Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights*, [2001] CRIMINAL LAW REVIEW at 73-91, <<http://www.cyber-rights.org/documents/crimlr.pdf>> (date accessed: October 14, 2002)

<sup>18</sup> See JUSTICE, *Regulation of Investigatory Powers Bill* (London, 2000), <<http://www.justice.org.uk/images/pdfs/powerbill1.pdf>> (date accessed: October 14, 2002)



*Investigatory Powers Act*<sup>19</sup> and its amendments. The U.K. Information Commissioner was also highly critical of the Act.<sup>20</sup> The resultant delays and last minute changes attest to the controversial nature of such legislation.<sup>21</sup>

In this connection, we emphasize that neither the *Convention*<sup>22</sup> nor the Proposal itself is empirically justified. The Proposal speaks broadly of the need to combat cybercrime, but offers no factual basis for believing that existing law is inadequate. Have any important investigations been frustrated because law enforcement officials lack these proposed powers? What kind of investigations? How many? What percentage?

Nor does the Proposal provide means for evaluating whether, if adopted, it will have actually aided law enforcement in fighting cybercrime without unduly sacrificing Canadians' privacy rights. Indeed, the *Convention* expressly requires that Parties obligate service providers to "keep confidential the fact of and any information about the execution of any power" provided for in Articles 20 and 21, with no durational limit.<sup>23</sup> Such provisions hinder the accountability necessary both before and after a free and democratic society expands its domestic surveillance power. As the Supreme Court has said, s. 8 "requires a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred."<sup>24</sup>

In addition, surveillance of communications implicates not only the right of privacy, but also the s. 2 freedoms of expression and association. This is true not only for one's conversations, whether by telephone or e-mail, but also for the many other informational functions of the Internet such as researching, reading, or working with others on writings or political, religious, and cultural activities. Of particular concern here is the broad working definition of "service provider," which clearly includes universities, colleges and libraries that provide Internet access to the public.<sup>25</sup>

Given the importance of these constitutional rights, especially the right to be free from unreasonable search and seizure (and its peculiar vulnerability to covert abuse), civil liberties must be given paramount consideration before changing Canadian law. Strict limits on law enforcement powers are required in order to protect the civil liberties of Canadians. Law enforcement officials do not have an inherent right to search and seize information for whatever purpose they see fit. Government objectives, no matter how apparently noble and pressing, cannot escape the reasonableness inquiry demanded s. 8: "assessment of the constitutionality of a

---

<sup>19</sup> (2000), c. 23.

<sup>20</sup> See Data Protection Commissioner, *Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill*, <[www.fipr.org/rip/DPCparlRIP.htm](http://www.fipr.org/rip/DPCparlRIP.htm)> (date accessed: October 14, 2002), S. Millar, "Snooping Laws May Be Illegal", *The Guardian*, July 31, 2002, <<http://www.guardian.co.uk/internetnews/story/0,7369,766703,00.html>> (date accessed: October 14, 2002).

<sup>21</sup> "Blunkett Abandons Big Brother", BBC News, June 18, 2002, <[http://news.bbc.co.uk/1/hi/uk\\_politics/2051670.stm](http://news.bbc.co.uk/1/hi/uk_politics/2051670.stm)> (date accessed: October 14, 2002).

<sup>22</sup> See generally Ryan Baron, Comment, *A Critique of the International Cybercrime Treaty*, 10 COMMLAW CONSPECTUS 263, 265-267 (2002) (describing history of convention).

<sup>23</sup> *Convention*, Article 20, ¶ 3 (real-time collection of traffic data); id. at Article 21, ¶ 3 (interception of content data).

<sup>24</sup> *Hunter*, at 160.

<sup>25</sup> Proposal, at 4 (provisionally defining "service provider" as "a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada").

search and seizure . . . must focus on its 'reasonable' or 'unreasonable' impact on the subject of the search or the seizure, and not simply on its rationality in furthering some valid government objective."<sup>26</sup>

### 3. Intercept Capability Requirement

#### a. Should There Be a Requirement of Intercept Capability?

The Proposal would require all service providers to ensure communications intercept capability. As a preliminary matter, this requirement appears unnecessary in order for Canada to comply with the *Convention*. Nor is there any indication that this requirement is necessary to law enforcement, either in the sense that important investigations have been hindered or impaired without it, or that technological changes will make such impairment likely in the future. On this basis alone, the requirement of intercept capability should be rejected.

More fundamentally, the intercept capability requirement would be a major step toward an undesirable and unwise government-telecommunications industry "surveillance partnership." In unprecedented fashion, the government would be in a position to wield great influence over the design and operation of modern telecommunications. Such a partnership raises significant issues of proportionality and accountability, especially in light of how individuals use the Internet to learn and to speak about matters of personal importance to them. As the Supreme Court has recognized, "privacy concerns are at their strongest when aspects of one's individual identity are at stake, such as in the context of information about one's lifestyle, intimate relations or political or religious opinions."<sup>27</sup> Medical and health privacy issues must also be recognized as more medical information is electronically transmitted and as doctor-patient communications take advantage of new communications technologies.<sup>28</sup>

A public/private surveillance partnership raises proportionality issues because both government and business have strong incentives to use surveillance technology. Government, of course, wants access to personal information for efficiency reasons and for broader public policy purposes like national security and law enforcement.

Business, meanwhile, wants personal information for marketing and efficiency reasons. In the Internet context, technologies like "cookies" and "Web bugs" only exacerbate the privacy problems associated with the inherent traceability of Internet activity. For instance, on the Internet one can hardly protect one's privacy in commercial transactions by using cash. Even non-commercial Internet activity, such as reading documents on Web pages, invariably requires the transmission of IP address information that can unambiguously identify what one reads. The Supreme Court in *Dyment* observed that "[c]ertainly, physicians, hospital employees and other health-care workers ought not to be made part of the law enforcement machinery of the state."<sup>29</sup> The same principle applies to telecommunications, which for the modern user is, among other things, a library, a telephone and a printing press.

The danger here is that a public/private surveillance partnership will lead to individuals' being increasingly watched by unseen entities. As our lives become increasingly tied to the electronic media and computers, from ubiquitous cellular telephones to public video cameras to biometric scanning devices, more and more of our daily activity is subject to scrutiny by one or

---

<sup>26</sup>*Hunter*, at 109.

<sup>27</sup>*R. v. Mills*, [1999] 28 C.R. 207, 251.

<sup>28</sup>See *Dyment* at 432-433 (trends in health care exacerbate medical privacy problems).

<sup>29</sup>*Dyment*, at 433-434.

both of these surveillance partners. Every website we visit, every e-mail we send, every purchase we make, perhaps every step we take, may be recorded permanently. The uncertain prospect of such covert and detailed surveillance will, for many, create tremendous pressures toward social conformity. Individuals will be more wary of reading about controversial cultural, social, political and religious ideas for fear that they will be subjected to surveillance. A report commissioned by the European Parliament's Civil Liberties Committee noted that while surveillance technologies are justified under state interest rationales, they are often used to monitor political dissent, journalists, minorities and political opponents; the report concluded that surveillance technologies have a chilling effect on those who may wish to take dissenting viewpoints and protest government policy.<sup>30</sup>

At the same time, a public/private surveillance partnership makes it more difficult to hold state agents accountable for their actions. Government can sit, like an innocent bystander, while businesses gather personal information; then, under reduced legal standards, collect that detailed information. The problem is that when the government is intimately involved in the operation and design of telecommunications or computer systems, individuals have no easy way to know whether and how the privacy of the commercial systems they use for communicating have been affected by government requirements. Nor will they know how the government makes use of its new power.

In terms of promoting intercept capability, the stated goal of the Proposal is to make it feasible for law enforcement to intercept, "subject to a lawful authority," the content and related data associated with any communication. This general mission statement raises at least three privacy concerns. First, to safeguard the rights of citizens, any legislation authorizing intercept capability for new technology should specify what kind of "lawful authority" is necessary before the interception capability can be used. Second, if government is to require all telecommunications providers to build in interception capability, it should specifically state what legal standards govern the interception of different kinds of communications data. Third, given the broad working definition of "service provider," universities, colleges, and libraries will all be affected.

First, the Proposal specifies that intercept technology will include the ability to intercept the content of communications in addition to the complete range of communications associated data. Accordingly, it is essential that government specify what type of lawful authority is needed before interception can occur. Canadian law treats different aspects of communications differently. For example, a lower showing is required for law enforcement to obtain a list of the telephone numbers an individual dials than for the content of a communication. In emerging communication media, there will be a range of communication attributes, some of which will be similar to telephone numbers in the quantity of information they are capable of revealing, some of which will clearly be communications content, and others of which will fall somewhere in between. For example, the name of a file attached to an e-mail has both attribute and content characteristics.<sup>31</sup> Another important issue is so-called "location" data, such as the location of a cellular telephone user. Government must specify what "lawful authority" means before information conveyed through new media can be intercepted. As the Supreme Court has noted, "where privacy is outweighed by other societal claims, there must be clear rules setting forth the

<sup>30</sup>See European Commission's Science and Technology Options Assessment Office, *ASSESSING THE TECHNOLOGIES OF POLITICAL CONTROL* (1997).

<sup>31</sup> See generally Susan Freiwald, *Uncertain Privacy: Communication Attributes after the Digital Telephony Act*, 69 S.CAL.L.REV. 949 (1996).

conditions on which it can be violated. This is especially true of law enforcement, which involves the freedom of the subject.”<sup>32</sup>

Second, any legislation should address the necessary standard of review for specific kinds of communications attributes, and should explicitly forbid the interception of others without prior legislative action. The government should not simply analogize to more established media and proclaim that law enforcement capability to intercept communications in new media should be identical, for a standard that is appropriate to one medium may not translate well to another. This would involve giving substantive thought to issues such as the ways in which communication in new media differ from communication through traditional media, and resolving how law enforcement should treat these differences. A thoughtful legislative process would allow Canada to avoid the difficulties that have befallen other nations engaged in the implementation of interception requirements.

For example, the United States in 1996 enacted the Communications Assistance to Law Enforcement Act (“CALEA”). Like the Proposal, CALEA’s stated purpose was to require communications carriers to make it technically feasible for law enforcement to intercept communications.<sup>33</sup> CALEA was not intended to modify the regime governing what kinds of information law enforcement could access. Rather, the purpose was to ensure that law enforcement could monitor new communications media to the same extent as traditional media such as the ground-line telephone.<sup>34</sup>

CALEA implementation in the United States gave rise to a number of problems that Congress had not explicitly considered, leading to years of protracted litigation. One general problem concerned how, as a technological and engineering matter, CALEA should be implemented. The telecommunications industry negotiated for several years with the Federal Bureau of Investigation (“FBI”) over industry design standards.<sup>35</sup>

Another general problem was privacy. The proposed industry standard was rejected by U.S. law enforcement agencies because the FBI wanted nine capabilities omitted by the industry standard.<sup>36</sup> Of particular contention were whether telephone companies were obligated to give law enforcement information concerning the nearest antenna tower through which calls were located, thus helping law enforcement pinpoint the physical location of individuals being monitored, and information about numbers dialed *after* an initial call was made, such as call forwarding, accessing voicemail, etc. Because these issues were not addressed by Congress, it was ultimately up to the courts to surmise Congressional intent.<sup>37</sup> Resolving these issues at a legislative level would permit meaningful public participation in making these important distinctions. Allowing courts to draw these distinctions is a de facto delegation of these decisions to the judicial branch. These issues are even more important for the Proposal than for CALEA, because CALEA does not apply to ISPs.

Further, the cost issue for interception capability is one that should not be considered lightly, given the financial difficulties that have plagued the Canadian telecommunications industry in recent years and the experience of other countries. The example of the Netherlands

<sup>32</sup>Dymont, at 430.

<sup>33</sup>Unlike the Proposal, however, CALEA does not apply to Internet service providers.

<sup>34</sup>H.R. Rep. No. 103-827, pt. 1, at 9 (1994).

<sup>35</sup>Jason Broberg, Comment, *From CALEA to Carnivore: How Uncle Sam Conscripted Private Industry in Order to Wiretap Digital Telecommunications*, 77 N.DAK.L.REV. 795, 796 (2001).

<sup>36</sup>Id. at 796-802.

<sup>37</sup>See *U.S. Telecom Association v. Federal Communications Commission*, 227 F.3d 450 (D.C. Cir. 2000).

should be kept in mind. The Netherlands passed legislation requiring interception capability for which service providers were to bear the costs. ISPs were first given until August 2000, then until April 15, 2001, to comply with the regulations. However, in February 2001, the ISPs complained that the deadline was unrealistic and argued that the specifications for interception capabilities were not clear and up to one third of Dutch ISPs could face bankruptcy from implementing such interception capabilities.<sup>38</sup> The deadline was thus again pushed back as ISPs agreed in May 2001 to form an organization that would manage the interception equipment within six to nine months.<sup>39</sup> Similarly, in the United States, CALEA remains less than fully implemented after eight years partly because of disagreement over cost recovery.<sup>40</sup> Cost issues typically affect small providers far more than large providers.

Finally, we note that any requirement of interception capability is likely to hinder the ability of the telecommunications industry to innovate and offer new services. It is dubious industrial policy to permit law enforcement to intrude upon technological design choices.

Third, we question whether the drafters of the Proposal have given any thought to how universities, colleges and libraries would be affected. Many of these institutions, which by tradition are open environments devoted to research inquiry, offer anonymous public Internet access terminals. Under the Proposal, libraries and academic institutions would apparently be required to keep track of Internet users and the sites they visit.

#### **b. E-Mail Interception Concerns**

The Proposal asks for a clarification of the legal status of e-mail, for the purpose of determining whether the capture of an e-mail falls within the scope of Part VI of the Criminal Code, which criminalizes the interception of a private communication, or whether it merely constitutes a search or seizure.

Judicial authorization of the interception of a private communication requires the Crown to meet a higher threshold than is required for a warrant for a search and seizure. The Ontario Court of Appeal aptly described the rationale for this higher threshold in *R. v. Finlay*:<sup>41</sup>

"It is also apparent that, although an analogy may be drawn between judicial authorizations to intercept private communications and judicial authorizations for conventional search warrants, there are substantial differences between the two

---

<sup>38</sup> J. van Buuren, "Interception Requirements Get Dutch Internet Providers Into Trouble", *Telepolis*, February 15 2001, <<http://www.heise.de/tp/english/html/result.xhtml?url=/tp/english/inhalt/te/4932/1.html>> (date accessed: October 14, 2002).

<sup>39</sup> J. van Buuren, "Dutch Government and ISP's Reach Compromise On Interception of The Internet", *Telepolis*, April 25, 2001, <<http://www.heise.de/tp/english/html/result.xhtml?url=/tp/english/inhalt/te/7458/1.html>> (date accessed: October 14, 2002).

<sup>40</sup> Jeffrey Yeates, *CALEA and the RIPA: the U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 ALB.L.J. SCI. & TECH. 125, 143-146 (2001). For the most recent description of CALEA's status, see U.S. Department of Justice, Federal Bureau of Investigation, *CALEA Implementation Section, Communications Assistance for Law Enforcement Act, Flexible Deployment Assistance Guide* (3rd Ed. May 2002).

<sup>41</sup> (1985), 23 C.C.C. 93d) 48, 48 C.R. (3d) 341 (Ont. C.A.), leave to appeal to S.C.C. refused [1986] 1 S.C.R. ix.

types of authorizations. A search warrant authorizes the search of specified premises for specific things already in existence. The person executing a search warrant will normally know whether a particular item found on the searched premises comes within the scope of the warrant. A search warrant authorizes a single entry of the premises to be searched, and if the items sought are not found, an application for a second search warrant must be made in order to make a further entry. In contrast, an authorization to intercept private conversations authorizes the interception of conversations which have not yet taken place. The interception may occur at any time during the period specified in the authorization. It will often be the case that the listener will not be able to determine whether the intercepted conversation constitutes the evidence sought until after he has heard it in its entirety in the context of other conversations similarly overheard."<sup>42</sup>

### c. The Legal Status of the Capture of E-Mail

The leading case on the legal status of e-mails is the Alberta Court of Appeal decision in *R. v. Weir*,<sup>43</sup> where the Court found that e-mails fell squarely within the definition of "private communication"<sup>44</sup> in Part VI of the Criminal Code, and that prior judicial authorization was required to search or seize e-mails.<sup>45</sup> Any legislative attempts at clarifying the legal status of e-mail must provide to e-mail a level of protection at least equivalent to that granted by the courts.

The Proposal asks some questions about what constitutes an "interception" of an e-mail. It argues that the capture of an e-mail in transit or waiting to be delivered would probably constitute an interception, while the acquisition of an e-mail stored at the sender or receiver's ISP would likely constitute a seizure. However, "intercept" is defined in the Criminal Code as "listen to, record or acquire a communication or acquire the substance, meaning or purport thereof." The capture of an e-mail falls within that definition because capturing an e-mail captures its contents, whether or not it is in transit. Moreover, because of the "store and forward" nature of e-mail and other Internet communications, any rule that distinguishes e-mail in transit from stored e-mail would fail to protect communications privacy because law enforcement need only wait until the e-mail transmission ends.

In any case, the *Finlay* rationale for applying a stricter authorization standard for interceptions than for seizures extends to the capture of e-mails, regardless of whether they are stored or in transit. Law enforcement officials will generally have only a broad idea of what they are looking for and will need to read many e-mails to determine if they have found what they are

<sup>42</sup>*Ibid.* at 547-548.

<sup>43</sup> [1998] A.J. No. 155, *aff'd* [2001] A.J. No. 869 (C.A.).

<sup>44</sup> Part VI of the Criminal Code defines "private communication" as:

"any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it."

<sup>45</sup> *Weir*, at para. 70.



looking for, just as they do for telephonic interceptions. We therefore urge that the capture of e-mail be treated as an interception regardless of whether the e-mail is stored or in transit.<sup>46</sup>

#### **4. Production Orders**

##### **a. Should There Be a Specific Power to Allow Access to Traffic Data?**

The Proposal calls for the creation of a specific production order under a lower standard to access traffic data. We strongly urge the government to reject any legislation that would allow law enforcement to obtain "telecommunications associated data" (TAD) under a reduced standard. The Proposal portrays TAD as having little privacy value, arguing that it should be subject to the same reduced standard that applies to Dialed Number Recorders (DNRs). The analogy drawn between TAD and data captured by DNRs is false and should be rejected. TAD reveals substantially more about individual activity than does the use of a DNR.<sup>47</sup> Allowing government access to this data without the normal showing would significantly erode privacy.

First, the scope of what will constitute TAD is not analogous to what is captured by a DNR. DNRs capture the telephone number of the caller, the person called, and the duration of the call. Under the extremely broad definition of TAD, the information that would be captured at a lower standard would be much broader. At a minimum, this would include: the IP address of the computer from which an e-mail was sent; the e-mail address from and to which the communication was sent<sup>48</sup>; the date and time of a communication; the duration of the communication, e.g., the time it took for the e-mail to be transmitted from sender to receiver; and the size in bytes of the communication. As currently defined, TAD also probably includes features of the e-mail that skirt the content/attribute divide, such as the subject line of an e-mail and the name of a file attached to an e-mail. Finally, the broad and vague definition employed strongly indicates that the addresses of the Web sites one visits are also TAD.

The expansive scope of the definition of TAD brings us to the second reason to reject the DNR analogy: the scope of data captured under the definition translates into a more invasive law enforcement tool. Under this definition, the range of human activity that will be subject to government observation through capture of TAD is substantially greater than that gleaned by using a DNR. A list of Internet sites visited, for example, will provide law enforcement with knowledge of the subject matter one reads, often specifying the exact document that resides at a particular IP address or URL. Knowing whether an e-mail contains an attachment, and if so, what type of attachment, allows law enforcement to glean more detailed information about what one is doing than is apparent through knowledge of the phone number one dials or is dialed by. Because of the revealing nature of the non-content information that accompanies Internet activity, a lower standard is unwarranted.

Third, TAD pinpoints communications by particular individuals with much greater precision than can be done using a DNR. A telephone number is a fairly weak link to particular

---

<sup>46</sup>Only if the e-mail has actually been opened by the recipient but remains stored on the provider's system is there even a plausible argument that the capture is a seizure and not an interception. But on this argument, law enforcement should only be able to use the seizure standard after a factual showing that the e-mail had, in fact, been opened.

<sup>47</sup>For a detailed exploration of this argument, see Freiwald, *supra* n. 31.

<sup>48</sup>"Since almost all user accounts require a password for access, knowing that a person's user ID sent a particular transmission gives presumptive knowledge as to the identity of the party originating that communication." Freiwald, *supra* n. 31, at 955.

individuals, because anyone who can dial a phone can use it. In contrast, an Internet communication is generally linked to a password protected account that is more likely to be used by one identifiable individual. This means that law enforcement access to telecommunications associated data poses a substantial privacy risk, rendering a reduced standard unjustifiable.

Fourth, TAD is primarily interesting to law enforcement because it allows law enforcement to make inferences about content, or even to determine with certainty what content has been communicated. The latter situation is obvious given that many IP addresses or URLs point to specific documents. Once law enforcement officials capture the URL, they can go to that URL and see exactly what content was read. This fact, combined with other technological capacities that did not exist in the days when DNRs were cutting edge, like the capacity to store and mine vast amounts of data, means that law enforcement access to TAD without a standard showing opens the door to the possibility of the general search. Without having to show reasonable grounds that an offense has been or will be committed, law enforcement could collect huge quantities TAD and search for what is perceived as suspicious activity. This practice could have a substantial, negative impact on the willingness of individuals to participate in the online marketplace of ideas.

Finally, a definition of what should be accessible under a lower standard should be *narrower* online than on the standard telephone, because so much more human activity takes place online than over the telephone. Internet activity is not limited to one-on-one or small group communication. Internet users can associate in large groups to advance political causes, can join anonymous support groups to discuss addictions or other ailments without fear of social stigma, or can simply read about whatever topic comes to mind from the privacy of their own homes. Allowing government to access detailed electronic records about these activities without even making the standard showing poses a substantial threat to the development of this dynamic new medium as a forum for the exchange of ideas and information. In order to ferret out the few who use new communications mediums for criminal activity, the Proposal deprives the millions of law-abiding Internet users in Canada of the normal safeguards of the law.

Prior to the legislative intervention which resulted in the enactment of s. 492.2 of the Criminal Code, some courts found that the use of a DNR to obtain local call information without judicial authorization contravened Part VI of the Criminal Code since it constituted an interception of a private communication,<sup>49</sup> while other courts concluded otherwise.<sup>50</sup> Collecting information with DNRs is therefore already close to the line between interception of private communications and ordinary search and seizure. For the reasons outlined above, that line is crossed by traffic data, which is clearly more private than information collected by DNRs. Hence, traffic data falls within the definition of "private information" under Part VI of the Act and should only be accessed through an interception authorization.

Quite independently of whether TAD should be captured under a lower standard, the government must specify what, exactly this means. Simply declaring that law enforcement surveillance capacity in new media should "equal" those in the telephone context is not enough, because it is rarely obvious what, substantively, this would entail. For example, some features of new media seem to fall between the cracks of "content" and "non-content" information, like the name of a file attached to an e-mail, or the subject line of an e-mail. Under the *Convention's* "principle of proportionality," Parties should distinguish between different types of traffic data

<sup>49</sup> *R. v. Griffith* (1988), 44 C.C.C. (3d) 63 (Ont. C.A.); *R. v. Khiamal*, [1990] A.J. No. 279 (Q.B.); *R. v. Mikituk*, [1992] S.J. No. 235 (Q.B.) [hereinafter *Mikituk*].

<sup>50</sup> *R. v. Samson* (1983), 45 Nfld. and P.E.I.R. 32 (Nfld. C.A.); *R. v. Beck*, [1993] B.C.J. No. 1141 (S.C.).



according to their sensitivity.<sup>51</sup> In other words, government should specifically address new media and state what non-content data can be collected at the lower level of protection.

**b. Should There Be a Specific Order for Subscriber/ Service Provider Information?**

The Proposal proposes production orders allowing law enforcement agencies to obtain subscriber information (such as name, billing address, phone number and name of service provider) without prior judicial authorization. There would be no prior judicial oversight of law enforcement officials' collection of such personal information. A warrantless search is presumed to be unreasonable and violate s. 8.<sup>52</sup> The importance of prior judicial authorization when privacy interests are at risk cannot be overemphasized, given that breaches of privacy often cause irreparable harm:

"[I]f the privacy of the individual is to be protected, we cannot afford to wait to vindicate it only after it has been violated. This is inherent in the notion of being secure against unreasonable searches and seizures. Invasions of privacy must be prevented, and where privacy is outweighed by other societal claims, there must be clear rules setting forth the conditions in which it can be violated. This is especially true of law enforcement, which involves the freedom of the subject."<sup>53</sup>

The Proposal argues that access to subscriber information without prior judicial authorization merely codifies the current practice of service providers. This is false. Under the CRTC Telecom Decision CRTC 2002-21,<sup>54</sup> which sets forth the requirements for law enforcement agency access to the identity of the local service provider (LSPID) associated with a telephone number, a law enforcement agency must identify its lawful authority to obtain the information and show either that:

- (i) it has reasonable grounds to suspect that the information relates to national security, the defence of Canada or the conduct of international affairs;
- (ii) the disclosure is requested for the purpose of administering or enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing or administering any such law; or

<sup>51</sup> *Convention*, Article 15, ¶ 1; see also Explanatory Report to the Convention on Cybercrime, ¶ 31 ("The definition leaves to national legislatures the ability to introduce differentiation in the legal protection of traffic data in accordance with its sensitivity. . . . the substantive criteria and the procedure to apply to an investigative power may vary according to the sensitivity of the data.") <<http://conventions.coe.int/Treaty/en/Reports/HTML/185.htm>>.

<sup>52</sup> *Hunter v. Southam*, [1984] 2 S.C.R. 145.

<sup>53</sup> *Dyment*, supra note 1 at para. 23.

<sup>54</sup> Telecom Decision CRTC 2002-21: Provision of subscribers' telecommunications service provider identification to law enforcement agencies (April 12, 2002), <<http://www.crtc.gc.ca/archive/ENG/Decisions/2002/dt2002-21.htm>> (date modified: April 12, 2002).

(iii) it needs the information because of an emergency that threatens the life, health or security of an individual, or the LEA otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals and property.<sup>55</sup>

These requirements for LSPID disclosure are quite strict (and would not include contacting next-of-kin in emergency situations). Further, "LSPID reveals nothing about the identity or activities of the subscriber related to the telephone number,"<sup>56</sup> and is thus far less revealing than subscriber information, which includes name, billing address, and phone number. Hence, the disclosure of subscriber information should be subject to a higher standard than that required for the disclosure of LSPID.

Furthermore, the practice of disclosing subscriber information likely contravenes s. 8 of the Charter. In *R. v. Plant*,<sup>57</sup> the majority of the Supreme Court found that police search of computerized records of household electricity consumption did not require a warrant because there was no reasonable expectation of privacy in that information. However, the majority decision was tempered by the strong dissent by Madame Justice McLachlin, which argued that the records were subject to a reasonable expectation of privacy. Both sides agreed that this case was "close to the line."<sup>58</sup> The majority based its decision in part on the fact that the information was available to the public, while McLachlin disagreed and stated the information was not publicly available. She recognized the importance of the right to privacy in computerized information:

"Computers may and should be private places, where the information they contain is subject to the legal protection arising from a reasonable expectation of privacy. Computers may contain a wealth of personal information. Depending on its character, that information may be as private as any found in a dwelling house or hotel room."<sup>59</sup>

If the information in *Plant* was "close to the line," subscriber information that relates to one's communications clearly crosses that line. In this day and age, we have come to recognize the sensitive nature of information held in computers (such as financial information), and that information held in a computer is not necessarily publicly available. We have also passed additional privacy legislation, the *Personal Information and Protection of Electronic Documents Act*<sup>60</sup> (PIPEDA), which protects personal information held by private entities such as communications service providers. It is time that we fully recognize the personal nature of subscription and billing information held in computers, and the need for prior judicial authorization for state access to that data. In Europe, Article 6 of the EU Directive on the Protection of Privacy in the Telecommunications<sup>61</sup> provided that traffic and billing data had to be erased or anonymized as soon as the billing period ended. Based on this Directive, the UK Data

---

<sup>55</sup> *Ibid.*, at para. 22.

<sup>56</sup> *Ibid.*, at para. 12.

<sup>57</sup> [1993] 3 S.C.R. 281.

<sup>58</sup> *Ibid.*, at paras. 33, 41.

<sup>59</sup> *Ibid.*, at para. 45.

<sup>60</sup> S.C. 2000, c. 5.

<sup>61</sup> Directive 97/66/EC.

Protection Commissioner argued that access to billing data should be subject to judicial authorization.<sup>62</sup>

The Proposal also suggests that production orders should be available so that law enforcement officials could have access to subscriber information without a court order during the early stages of an investigation, or for non-investigatory purposes such as contacting next-of-kin in emergency situations. There are several concerns with such a policy, particularly one that would apply to information already in the possession of telecommunications providers. First, telecommunications providers often have privacy policies. If production orders mandate the handing over of more information than was permitted by these privacy policies, the privacy of individuals who relied on these policies will be violated, which could erode the value customers place in such policies. Second, knowing that information can be easily handed over to government authorities upon request will increase the likelihood that customers will simply give their telecommunications providers false information, thus decreasing the value and accuracy of such data.

Finally, we urge that no service provider ever be required to collect subscriber information that it does not collect for its own purposes. Such a requirement is a form of "data retention," which the *Convention* does not require and which the Proposal expressly distinguishes.<sup>63</sup> Based on comments made at the November 2 public hearing in Vancouver, it appears data retention is being discussed; if so, the public should be told. The retention of vast amounts of information, including complete clickstream traffic, would be a major expansion of the assault on privacy. Indeed, such a requirement would effectively make anonymous communications impossible.

##### 5. National Database of Subscriber Information

We urge rejection of the proposal of the Canadian Association of Chiefs of Police to establish a national database of subscriber information. This proposal amounts to the collection by the state of personal information prior to the commission of an offence, and constitutes an unjustifiable extension of police surveillance into the private domain of communications.

Such a database entails massive collection of data about individuals who are not and are unlikely ever to be under investigation. This sort of dragnet information collection is not based on any kind of particularized suspicion; rather, it is data collection on large numbers of people "just in case" it is useful someday. The proposal is inherently overbroad.

National databases are vulnerable to criticism on many other grounds. First, by storing large amounts of valuable personal information in a single place, the government would create a single point of vulnerability for those interested in unauthorized access to such information. This kind of basic demographic information is fodder for identity theft. For better or worse, basic demographic data such as names and address are often used to verify identity. So long as this is the case, aggregating this data in one convenient location will be potentially dangerous to the security of individual from identity theft.

Second, though government can assert benign purposes for wanting to aggregate large quantities of personal data, such as informing next of kin in emergency situations, there are many more uses to which such data can be put that are not at all benign. Specifically, the aggregation

---

<sup>62</sup> Data Protection Commissioner, *Response of the Data Protection Commissioner to the Government's Regulation of Investigatory Powers Bill*, <[www.fipr.org/rip/DPCparlRIP.htm](http://www.fipr.org/rip/DPCparlRIP.htm)> (date accessed: October 14, 2002) at para. 9.

<sup>63</sup> Proposal, at 14.

of large amounts of personal data is a prerequisite for government to engage in identity profiling. Using modern computer search technology, government will be able to construct profiles of those they think likely to commit or to have committed crimes, and then take advantage of large pools of personal data to search for individuals who match. This risk can be cut off before it becomes a threat by preventing law enforcement from amassing this kind of data to begin with.

Third, the establishment of a national database of subscriber information for law enforcers constitutes a blatant contravention of existing privacy legislation. The law enforcement officials with access to the database would infringe sections 4, 5 and 7 of the *Privacy Act*.<sup>64</sup> Section 4 provides that no personal information shall be collected by a government institution unless it relates directly to an operating program or activity of the institution, while section 5 states that government institution shall, wherever possible, collect personal information that is intended to be used for an administrative purpose directly from the individual to whom it relates. Section 7 of the *Privacy Act* provides that personal information shall not be used except for the purpose for which it was obtained, subject to the exceptions set out in s. 8(2) of the act. In addition to infringing specific provisions, the database would also clearly violate the spirit of the *Privacy Act*.

Indeed, the service providers disclosing the information for the purpose of establishing the database would be in breach of section 7(3)(c.1) of the *PIPEDA*, which sets out the requirement for the disclosure of personal information (defined as "information about an identifiable individual," which clearly includes subscriber information) to a government institution that has identified its lawful authority to obtain the information. Such disclosure is only permissible if the institution suspects the information relates to national security, is requested for the purpose of enforcing a law or carrying out an investigation, or is requested for the purpose of administering a law. The disclosure of subscriber information for all Canadians cannot fit within those three narrow requirements.

Finally, although the information that law enforcement now wants to collect sounds benign – after all, it is apparently limited to basic demographic facts — once a database of characteristics of individuals is established, there is no logical stopping point to indicate when data should cease to be accumulated. For example, government could articulate a paternalistic rationale to attempt to justify almost any type of data collection. Country of birth can also be seen as important to notifying next of kin in case of emergency. Since members of a particular ethnic group may be more likely to suffer from particular ailments, racial and ethnic identity could also potentially be added to the database. And so on. Once a government opens the Pandora's box of creating a database on its citizens, there is simply no logical end point. It is best to put the matter to rest before it begins.

The danger of "function creep" is especially serious given the apparent tendency of government today to establish large-scale "just in case" databases. An initiative of a similarly invasive scale is the recent CCRA proposal to establish a national database of every air traveller entering Canada, which has sparked massive criticism from the media and from privacy commissioners.<sup>65</sup>

The simultaneous proposals of these national databases are extremely worrisome, and warrant the "Big Brother" accusations with which they have been met. In both cases, the amount of data collected is unjustified, unprecedented and wholly unmanageable. It would be very difficult to keep such a large database secure from outside attacks. It is unclear what limits

<sup>64</sup> R.S.C. 1985, c. P-21.

<sup>65</sup> Privacy Commissioner of Canada, What's New, <[http://www.privcom.gc.ca/index\\_e.asp](http://www.privcom.gc.ca/index_e.asp)> (date accessed: October 14, 2002).

would be established on the uses of such information, and whether those limits would be respected, especially when combined with intercept capability requirements.

Indeed, the history of the CCRA proposal demonstrates how "function creep" can expand the scope of dataveillance — in the CCRA case, before the dataveillance program has even begun. Initially, the CCRA intended solely to identify incoming passengers whose records suggested that they were likely violate customs regulations, and target those passengers for secondary screening. Advance Passenger Information and Passenger Name Record (API/PNR) data for passengers not targeted for secondary screening would not be viewed by officials nor retained for more than 24 hours after the passenger's arrival in Canada.

But "the CCRA now intends to retain for six years the API / PNR information for all passengers entering Canada, whether or not the information is used for secondary screening or to make some other administrative decision. The CCRA intends to compile this information into a database and use it for a variety of purposes, including the detection of criminals, terrorists, and contraband. It also intends to make information in the database available to other government departments and institutions pursuant to recently amended provisions of the Customs Act."<sup>66</sup> Retired Supreme Court Justice Hon. Gérard V. La Forest concluded that the CCRA plan "would trench upon a reasonable expectation of privacy without either prior authorization or any measure of individualized suspicion. Government agencies would have access to detailed, travel-related information of millions of innocent Canadians. In my view this would violate section 8 of the Charter."<sup>67</sup>

In short, we agree with the views of the Privacy Commissioner of Canada, as stated in his Sept. 26, 2002 letter to the Minister of National Revenue:

"[T]he government of Canada has no business compiling databases of personal information about Canadians solely for the purpose of having this information available to use against us if and when it becomes expedient to do so. Such behavior violates the key principles of respect for privacy rights and fair information practices, and has no place in a free society."<sup>68</sup>

## **6. Data Preservation Orders**

The Proposal argues that data preservation orders are necessary by virtue of the *Convention*. Here again, we deem this argument weak because Canada has not yet ratified the *Convention*. Canada ought to be extremely wary about ratifying or following the *Convention*, as

---

<sup>66</sup>Opinion by retired Supreme Court Justice Hon. Gérard V. La Forest, C.C., Q.C., Appendix 1 to Privacy Commissioner of Canada, Letter to the Honourable Elinor Caplan, Minister of Revenue, November 22, 2002, <[http://www.privcom.gc.ca/media/nr-c/opinion\\_021122\\_1f\\_e.asp](http://www.privcom.gc.ca/media/nr-c/opinion_021122_1f_e.asp)> ((date accessed: December 16, 2002)).

<sup>67</sup>*Ibid*; see also Opinion of Mr. Roger Tassé (former Deputy Minister of Justice and Deputy Attorney General of Canada, 1977-1985), Appendix 2 to Privacy Commissioner of Canada, Letter to the Honourable Elinor Caplan, Minister of Revenue, November 22, 2002, <[http://www.privcom.gc.ca/media/nr-c/opinion\\_021122\\_rt\\_e.asp](http://www.privcom.gc.ca/media/nr-c/opinion_021122_rt_e.asp)> (arguing that CCRA database would be overbroad and disproportionate in violation of the right to liberty protected by s. 7 of the Charter) ((date accessed: December 16, 2002)).

<sup>68</sup>Privacy Commissioner of Canada, Letter to the Honourable Elinor Caplan, Minister of Revenue, September 26, 2002, <[http://www.privcom.gc.ca/media/nr-c/02\\_05\\_b\\_020926\\_e.asp](http://www.privcom.gc.ca/media/nr-c/02_05_b_020926_e.asp)> (date accessed: October 14, 2002):

it has been subject to strong criticisms from a variety of sources. For example, the drafting process has been widely criticized for its lack of openness and transparency. The process was completely secret until the 19<sup>th</sup> revision, and comments were only sought near the end of the drafting process.<sup>69</sup> Civil liberties groups have voiced dissatisfaction with the drafting process:

"The development of this Convention has been characterized by a lack of transparency and openness in relation to the CoE policy-making process. This process has been exceedingly secretive and has not benefited from any input except from selected law enforcement officials for several years. There have been no open meetings on this anywhere."<sup>70</sup>

Importantly, neither Article 16 nor Article 17 of the *Convention* is limited to criminal or other specific types of investigations. As one commentator has noted, there is a strong argument that both articles conflict with the protection principles of the E.U. Data Protection Directive, which asserted that data processing systems should be used to respect "fundamental rights and freedoms, notably the right to privacy."<sup>71</sup> "The argument is that without the proper procedural safeguards in place, a country could use the treaty as a means to enforce government policies unrelated to actual network intrusions, such as the identification and location of political dissidents. . . . A signatory could track, investigate and seize information in the investigation of other unfavorable policy decisions."<sup>72</sup>

This is especially important given the breadth of data covered by Article 16, which is not limited to communications or service providers. It applies to any data that has been stored in a computer system. Any business that uses a computer can be ordered to preserve any data that the government might want: Bank records, credit card data, inventory data, invoices, word processing, Web surfing data. A business that uses a video camera for surveillance can be told to preserve the tapes. The operator of an intelligent highway system or a passkey system can be required to preserve the data on the comings and goings of vehicles and people.

Therefore, we urge that the proposal for preservation orders be rejected. Requiring that any stored data be preserved, whether in electronic or paper form, is a significant intrusion upon privacy that must at least be justified by a specific and articulable factual showing made to a court that the stored data sought to be preserved is relevant to a specific investigation of a crime. Such minimal limits are consistent with the *Convention*, which provides that Article 16 and 17 powers "shall . . . include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration."<sup>73</sup>

In addition, in implementing the *Convention*, Canada should take care at the very least to respect the *Convention's* own safeguards. Article 16 stipulates that member states are to adopt

<sup>69</sup>See Baron, *supra* n. 22, at 265-267.

<sup>70</sup> Privacy International, *A Draft Commentary on the Council of Europe Cybercrime Convention*, October 2000, <<http://www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf>> (date accessed: August 14, 2002) at 5.

<sup>71</sup>Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), 31 at P2, available at [http://europa.eu.int/eur-lex/en/lif/dat/1995/en\\_395L0046.html](http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html).

<sup>72</sup>Baron, *supra* n. 22, at 275.

<sup>73</sup>*Convention*, Article 15, ¶ 2; see also *id.* at ¶ 3 (providing for Party consideration of "rights, responsibilities and legitimate interests of third parties").



legislative measures enabling competent authorities to make orders for data preservation for a maximum of 90 days. However, two of the proposed periods of preservation in the Proposal exceed this limit (120, 180 days).

The preservation of data should also be subject to additional safeguards. Data preservation harms the privacy of users, and decreases the security of the system by creating new vulnerabilities.<sup>74</sup> At the strictest minimum, there should be a requirement of confidentiality of the preserved data on the holder of the data, as stipulated in Article 16 of the *Convention*. The European Data Protection Commissioners have recommended the following safeguards in implementing data preservation: prior judicial authorization, notification of individuals, limits on use, record keeping requirements, monitoring and auditing, and public reporting.<sup>75</sup> Additionally, there is no mention in the Proposal of what ought to be done about the costs of data preservation. Preservation of data incurs costs to service providers due to storage and security concerns.

## 7. Conclusion

EFC and EFF hope that these comments will help the government recognize the importance of protecting individuals from privacy-invasive law enforcement actions. In issuing a finding that video surveillance in public places was unlawful, the Privacy Commissioner of Canada aptly noted that "[j]ust because something is technologically possible, that does not mean it is socially justifiable or acceptable."<sup>76</sup>

As a final word, we would like to stress the importance of refusing to accept the tensions between privacy and security as a zero-sum game. Adopting this attitude concedes too much to those who promote empowering law enforcement at any cost. Instead, a truly responsive legislature would seek creative solutions that accommodate both the values of security and of privacy. Given the ever-expanding horizon of technological possibility, the job of preserving privacy falls more and more to democratic institutions. Only by engaging in strong oversight of law enforcement action will Canada continue to embody the ideals set forth in the *Charter of Rights and Freedoms*.

Respectfully submitted,

---

<sup>74</sup> Privacy International, *A Draft Commentary on the Council of Europe Cybercrime Convention*, October 2000, <<http://www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf>>

<sup>75</sup> Retention of Traffic by Internet Service Providers (ISPs), European Data Protection Commissioners Conference 6/7 April 2000 Stockholm, <[http://www.datenschutz-berlin.de/doc/eu/konf/00\\_db\\_en.htm](http://www.datenschutz-berlin.de/doc/eu/konf/00_db_en.htm)>

<sup>76</sup> Letter of Finding from Privacy Commissioner of Canada, to David Loukidelis, Information and Privacy Commissioner of British Columbia (Oct. 4, 2001) (regarding video surveillance activities by the Royal Canadian Mounted Police in Kelowna, B.C.).

Electronic Frontier Canada  
20 Richmond Avenue  
Kitchener, Ontario  
N2G 1Y9

By:

[REDACTED]  
Dept. of Computer Science  
McMaster University  
Hamilton, Ontario  
[REDACTED]

[REDACTED]  
Dept. of Computer Science  
University of Waterloo  
Waterloo, Ontario  
[REDACTED]

[REDACTED]  
Dept. of Computer Science  
University of British Columbia  
Vancouver, British Columbia  
[REDACTED]

Electronic Frontier Foundation  
454 Shotwell Street  
San Francisco, California 94110

By:

s.19(1)

[REDACTED]  
Senior Staff Attorney  
+1 415 436-9333 x [REDACTED] (voice)  
+1 415 436-9993 [REDACTED] (fax)  
[REDACTED]



[REDACTED]

s.19(1)

--  
\*\*\*\*\*

[REDACTED]  
Professor  
Department of Computer Science  
2366 Main Mall  
University of British Columbia  
Vancouver, BC Canada V6T 1Z4  
Office: (604) 822-4142 FAX: (604) 822-5485  
E-mail: [REDACTED]  
\*\*\*\*\* \*\*

s.19(1)

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 16 5:03 PM  
To: 'la-al@justice.gc.ca'  
Subject: Lawful Access Consultation Document



Dec16\_lac.doc

2002/12/16 - Microcell Telecommunications Inc.

DESCRIPTION: Lawful Access Consultation Document - Released by the  
Department of Justice, Industry Canada and Solicitor General  
Canada on August 25, 2002  
- Comments of Microcell Telecommunications Inc.

FILENAME: Dec16\_lac.doc <<Dec16\_lac.doc>>

[REDACTED]  
Affaires réglementaires/Regulatory Affairs  
Microcell Telecommunications Inc.

Tel: (514) 937-0102, ext. [REDACTED]

Fido: (514) 992-4012

Fax: (514) 846-6928

Courriel/E-mail: [REDACTED]

December 16, 2002

**BY E-MAIL and REGULAR MAIL**

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, Ontario K1A 0H8

**Re: Lawful Access Consultation Document – Released by the Department of Justice, Industry Canada and Solicitor General Canada on August 25, 2002**

To whom it may concern,

We wish to inform you that Microcell Telecommunications Inc. ("Microcell") has received a copy of today's submission by the Canadian Wireless Telecommunications Association ("CWTA") on the above-noted subject, and we fully support the positions expressed therein.

We thank the Departments for the opportunity to comment on this matter, and remain,

Yours very truly,

(SGD) [REDACTED]

s.19(1)

[REDACTED]  
Vice-President, Regulatory Affairs  
Microcell Telecommunications Inc.

/des

cc: [REDACTED] CWTA

Pierlot, Paul

s.19(1)

---

**From:** [REDACTED]  
**Sent:** 2002 Dec 16 5:06 PM  
**To:** la-al@justice.gc.ca  
**Cc:** [REDACTED]  
**Subject:** SUBMISSION RE: LAWFUL ACCESS CONSULTATION  
**To:** Lawful Access Consultation  
Criminal Law Policy Section

Attached is FIRA's submission. Hard copy to follow by post.

Yours sincerely,

[REDACTED]  
Executive Director



BC FREEDOM OF  
INFORMATION  
AND PRIVACY  
ASSOCIATION

December 18, 2002

Lawful Access Consultation  
Criminal Policy Section  
5th Floor, 284 Wellington Street  
Ottawa, ON K1A 0H8

Dear Sirs/Mesdames:

**COMMENTS ON THE *LAWFUL ACCESS CONSULTATION DOCUMENT***

The B.C. Freedom of Information and Privacy Association ("FIPA") welcomes the opportunity to comment on the federal government proposals as set out in the *Lawful Access Consultation Document* ("Consultation Document").

FIPA is an organization devoted to the protection of Canadians' rights of privacy and access to information. Our objectives include defending the right to personal privacy enjoyed by the citizens of Canada. We also recognize the need of law enforcement and national security agencies to be able to work effectively to ensure a safe and secure society.

Please note that this submission has been prepared with input from, and has been endorsed by, a number of organizations who were unable to prepare their own submissions, but who wished to present their views to the federal government. These groups are listed at the end of this submission. FIPA sponsored two Vancouver workshops on the Lawful Access proposals workshops – the second in collaboration with Simon Fraser University's School of Communication – and received the input of over 45 groups and individuals.

In the context of telecommunications, Lawful Access is the interception of communications and the search and seizure of information carried out pursuant to legal authority as provided in Canadian law. The federal government proposes legislative amendments which are said, in part, to be required to ratify the Council of Europe *Convention on Cyber-Crime* ("Convention"), and to provide law enforcement agencies with the technical and legal capability to maintain lawful access when new technologies are used in connection with criminal activity.

We are opposed to the proposals in the Consultation Document, as they unjustifiably intrude upon the privacy rights of Canadian citizens.

## THE RIGHT TO PRIVACY

In analyzing proposals for access to information that intrude upon citizens' rights to privacy, one must start with Constitutional principles set out in the *Charter of Rights and Freedoms* ("The Charter"). The Charter guarantees citizens the right to be secure against unreasonable search or seizure, subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.

The right to privacy has long been recognized as one of the interests protected by s.8 of the Charter. In *Hunter v. Southam Inc.* [1984] 2 S.C.R. 145, the court held the purpose of s. 8 includes the protection of individuals' reasonable expectation of privacy. It limits government action that infringes on that right. In assessing those limits, the right of individuals to privacy must be balanced against the interest of government in law enforcement.

The right to privacy is important to our personal autonomy and the foundation of our democratic nation. As stated *R. v. Dyment* [1998] (S.C.C.),

Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.

In assessing proposals for electronic surveillance (such as are proposed in the Consultation Document), one must be mindful of the discussion of the majority of the court in *R. v. Duarte* [1990] 1 S.C.R. 30:

"I begin by stating what seems to me to be obvious: that, as a general proposition, surreptitious electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under s.8 of the Charter.

...

If one is to give s.8 the purposive meaning attributed to it by *Hunter v. Southam Inc.*, one can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance and to which, in consequence, the protection accorded by s.8 should be more directly aimed.

...

The reason for this protection [regulating the power of the state to record communications] is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful

- 3 -

residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communication will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning."

Any legislation that infringes citizens' rights to be free of unreasonable search and seizure must be reasonable and demonstrably justified. The onus of proving that a limitation meets that criteria is on the party seeking to uphold the limitation, in this case the Federal Government. As discussed in *R. v. Oakes* [1986] 1 SCR 103 two criteria must be met:

- (1) The objective of the legislation must be sufficiently important, pressing and substantial, "to warrant overriding a constitutionally-protected right"; and
- (2) The means chosen must be reasonable, demonstrably justified, and proportional, balancing the interests of society with those of the individuals. With respect to proportionality, the measures must be "rationally connected to the objective", and impair the right "as little as possible". Further, "there must be a proportionality between the effects of the measures... and the objective".

We agree with the Privacy Commissioner of Canada that any proposal that seeks to limit the right to privacy must meet a four-part test:

- it must be demonstrably necessary in order to meet some specific need;
- it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;
- the intrusion on privacy must be proportional to the security benefit to be derived; and
- it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.

---

<sup>1</sup> Letter to the Ministers responsible for the "Lawful Access" proposals, November 25, 2002.  
[http://privcom.gc.ca/media/le\\_021125\\_e.asp](http://privcom.gc.ca/media/le_021125_e.asp)

## SUMMARY OF CONCERNS AND RECOMMENDATIONS

Our concerns with the proposals contained in the *Lawful Access Consultation Document* can be summarized as follows:

1. The federal government seeks clarification with respect to the "private" status of e-mail, and suggests that "...[O]ne could argue that e-mail communications, as they are in writing, would not come within the 'private communication' definition."

We fundamentally disagree. We submit that e-mail is akin to a private oral communication. There is a high expectation of privacy in e-mail, and access to it should be obtained only under the high standard required for current lawful interception orders.

The future would be bleak indeed if Canadians had to communicate with the awareness that virtually any electronic conversation could be monitored and scrutinized by unseen government officials. Not only would our privacy rights be severely diminished, but our rights of freedom of expression as well.

2. The Consultation Document states that "The public policy objectives of this process are to maintain access capabilities for law enforcement and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada." However, the federal government proposals go beyond maintaining powers for new technology. The proposals greatly increase the breadth and depth of law enforcement agencies' powers to intercept, search and seize the private electronic communications and records of Canadian citizens.

In many cases, the powers proposed are unprecedented. In others, the powers proposed would substantially lower the threshold that is already required by Canadian law to obtain this information. This lower threshold does not adequately take into account the high degree of privacy that should be recognized in electronic communications and records.

3. The Consultation Document states that "These rapidly evolving technologies pose a significant challenge to law enforcement and national security agencies...as [they] can make it more difficult to gather the information required to carry out effective investigations." However, there is a lack of any empirical or other data that would demonstrate a pressing and substantial need for further law enforcement agency access to private electronic communications and records. There is little if any satisfactory justification given for the new powers proposed.



- 5 -

4. It is doubtful that the new powers proposed would be effective in enabling law enforcement and security agencies to keep up with technological innovations that are constantly being created. Lawbreakers will continue to find new avenues and methods of communication. If Canadians yield to what in fact are endless pressures to increase law enforcement surveillance powers, the result could be a huge loss of privacy in exchange for little gain in safety and security. In our opinion, we have a great deal to lose and not much to gain from the proposals.
5. The proposals in the Consultation Document are so vague in some instances that it is difficult to know what is being proposed. This makes it difficult to assess whether the proposals are reasonable, demonstrably justified and proportional.

We recommend the following:

1. Due to the high expectation of privacy in electronic communications and records, any proposed legislation should require a high threshold for lawful access commensurate with the expectation of privacy in those communications. Lower standards as discussed in the Consultation Document are not appropriate.  
  
The Criminal Code should be amended to clarify that e-mail, whether in transit or in storage, can be lawfully accessed only under this higher threshold.
2. As a necessary precursor of any legislation in this area, the government should present a well-argued system of privacy protection for private communications, that is not dependent on the form of the communication. The burden should not be placed on the average person to be careful in what he or she communicates because the medium they use determines a greater or lesser privacy status for that communication.
3. The federal government should provide a detailed statement and data with respect to the difficulties faced by law enforcement and national security agencies, so that the proposals for enhanced powers can be reviewed with that information.
4. The federal government should provide draft statutory wording with respect to the proposals, after taking into the account the concerns expressed in this and other submissions.
5. The public should have the opportunity to comment further on revised lawful access proposals, once 2 through 4 above have been completed.

## TECHNICAL INFRASTRUCTURE AND INTERCEPT CAPABILITY

The federal government proposes legislation that would require all service providers operating a "transmission facility" to ensure their systems have the technical capability to intercept communications.

The working definition of "transmission facility" is broad and would include wireless, wireline and Internet services. Existing systems would be grandfathered, and the requirement would only apply to new services or when there are significant upgrades to a system. The cost of compliance would be born by the service provider. There would be provisions for forbearance or exemption from the requirements under certain conditions.

Important Note: It is with surprise that we note that there is no provision in the *Convention on Cyber-Crime* that requires states to enact intercept capability legislation. Therefore, this proposal is not based on the Convention or any international requirement. We can only see this as a Canadian-made move for increased law enforcement powers. For all intents and purposes, *intercepts are wiretaps* and must be subject to all the thresholds and protections contained in Part XV of the Criminal Code and established jurisprudence.

Although the Consultation Document states that new services and technologies have "created difficulties", and make it "very difficult" to sustain the technical ability to lawfully intercept communications, no empirical or other data has been provided to adequately explain this. No information has been given as to how many investigations, if any, have been thwarted by cost in time or money because of lack of technical capability. No information is given as to why technical capability is required across all service providers. As a result, there is no evidence with which to assess whether there is a pressing or substantial need justifying this proposal and its effect on privacy rights.

### Universities, colleges, and public libraries

The definition of "service provider" is not sufficiently clear in the proposals. If the definition is to include institutions such as universities, colleges, and public libraries, there are serious concerns that such proposals will affect the ability of citizens to conduct anonymous communications and research. These are traditionally open and protected environments. Many libraries have workstations connected to the Internet that do not require IDs and passwords. The computer can be used anonymously. The proposals for data preservation orders and capture of customer name and address discussed below would not only create administrative difficulties for these bodies and its patrons, but also prevent any anonymous communications and research from being carried out. In the end, another important civil liberty would disappear.

- 7 -

We must be vigilant to ensure that increased intercept capability does not equate to a lowering of the standards for lawful access. Lawful access must continue to be obtained only by judicial warrant after a high threshold has been met.

## **GENERAL PRODUCTION ORDERS**

The federal government proposes creation of a "general production order" that would require third parties in possession or control of documents to produce the documents within a specified period of time.

Although there are very limited production orders in the Criminal Code, there is no such thing as a general production order. This is a new power and legal instrument that is being proposed. There is, however, existing provision for assistance orders which enable a judge to order that a person provide assistance in the execution of interceptions, warrants and certain orders.

For all intents and purposes, *production orders are warrants* and must be subject to all the thresholds and protections contained in Part XV of the Criminal Code and established jurisprudence. The federal government does not provide any empirical or other data to justify why a widening of such powers is necessary, or why the present search warrant combined with an assistance order is inadequate

The proposal would put the onus of conducting the search and production of the documents on the third party rather than having the search conducted by the law enforcement agency and assisted by the third party. In the absence of data, it is impossible to assess the justification for this power, and whether it is appropriate to conscript third parties to carry out law enforcement agencies' work.

## **ISPs should not be Agents of the State**

The proposed requirements on ISPs and other telecommunications providers to carry out actions mandated by the state continue a trend to co-opt private companies to become public agents of law enforcement officials. The job of ISPs and other like entities is to provide services for their customers. This should not include monitoring them for purposes of the state.

We disagree with the creation of a general production order. But if such a power were created, the threshold for obtaining one must be high, commensurate with the degree of privacy of the communications and records.

For example, if the order concerns the production of stored e-mail (see discussion below), the threshold should be the same as for the interception of private communications. Production orders must not be used to circumvent the high thresholds that would be required were the law enforcement agency to carry out the search or interception itself.

- 8 -

In addition, general production orders, if enacted, would require terms safeguarding the confidentiality and security of the information gathered for production.

### **Circumventing International Law Enforcement Procedures**

The Consultation Document states that production orders "could also allow law enforcement officials to obtain documents in cases where a search warrant cannot be delivered because the documents are stored in a foreign country". This statement raises concerns as to trans-border search of documents.

A Canadian search warrant cannot by itself be executed outside Canada to obtain documents that are not within the country. In those situations, mutual legal assistance procedures are employed. Production orders would effectively circumvent this procedure and the protections it provides for those within and outside Canada. The proposal is alarming as it raises the possibility of other countries expecting to be able to search computers in Canada with a foreign production order without going through the mutual legal assistance process.

### **"Anticipatory" Orders**

The Consultation Document also asks whether the Criminal Code should "allow for anticipatory orders (e.g., permit law enforcement agencies to monitor transactions for a specified period of time)".

No explanation other than the foregoing sentence is given as to what is meant by this proposal. No definitions of "anticipatory" and "monitor transactions" are given. No explanation or evidence as to why this is proposed is given.

The proposal must be rejected. If "anticipatory" implies that there is not yet sufficient evidence to meet the threshold to obtain an interception order or a search warrant, the proposal is a significant departure from existing law, and an unjustified intrusion of privacy rights. If "monitor transactions" means searching and seizing documents, existing law allows search and seizure under the threshold for judicial warrants. If "monitor transactions" means intercepting real time communication, then existing law allows such interception under Part VI of the Criminal Code, which has higher thresholds. Without more detail from the government it is impossible to comment further.

### **SPECIFIC PRODUCTION ORDERS FOR TRAFFIC DATA**

The government proposes a specific production order in the Criminal Code for "telecommunications associated data" ("traffic data"). A working definition of telecommunications associated data is given and includes "dialling, routing, addressing or signalling, that identifies...the origin, the direction, the time, the

- 9 -

duration or size...the destination or termination of a telecommunication transmission". The government further proposes that the threshold for such an order be the low standard that is currently required for production of telephone records and interception by dial number recorders.

Currently, the interception or search and seizure of traffic data may be ordered under the general warrant or interception provisions of the Criminal Code, both of which have higher thresholds. The proposal therefore calls for a carving out of traffic data from these provisions, and for the threshold for production of traffic data to be at a new lower standard. This obviously provides law enforcement agencies with greater powers of access.

The Consultation Document proposes a lower threshold for traffic data orders because of the "lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication". There is a fundamental error in the assumption of this statement. We submit that there is no lower expectation of privacy in an Internet address. To equate telephone numbers with Internet addresses ignores the considerable difference between the amount and quality of information that can be obtained from the two.

Information that can be obtained with an Internet address is far beyond what can be inferred or obtained from a telephone number. If a person telephones a department store to enquire about a product, all that may be recorded is the main number of the store. If the person were to visit the website of the store, and go to the web page of a department and then click on a product, several addresses would be generated, giving far richer information. Similarly, if a search engine is used, the search terms may be revealed in the address. The size of an e-mail may give information. Cellular phone records can identify the general location of the parties to the telephone call.

There is a high expectation of privacy in citizens' Internet and electronic communications. Monitoring this data is akin to video surveillance and interception of private communications. Presently the Criminal Code requires higher thresholds for lawful access for both of these, and that is the standard that should be adopted for an order for production of traffic data. The low standard for dial number recorders is not sufficient to protect the privacy rights of Canadians.

The Consultation Document also states that "a specific production order to be issued under a lower standard could also be created to obtain other data or information in relation to which there is a lower expectation of privacy". No details are given of what this "other data" may be, and it is impossible to comment on this aspect of the proposal, except to say that we fundamentally disagree with the constant theme in the Document that there is a lower expectation of privacy with respect to e-mail and other Internet-based communications.

- 10 -

## **ORDERS FOR SUBSCRIBER AND/OR SERVICE PROVIDER INFORMATION**

The Consultation Document suggests that there could be a specific production order for customer name and address (CNA) and local service provider identification (LSPID). Alternately, it proffers a proposal by The Canadian Association of Chiefs of Police that a national database of subscriber information be created or other existing databases be used to provide this information.

The Consultation Document does not provide satisfactory evidence or what pressing difficulty is being encountered by law enforcement agencies that would justify either of these proposals.

The proposal by the Chiefs of Police to establish a national database of subscriber information essentially amounts to the collection by the state of personal information prior to the commission of an offence, and constitutes an unjustifiable extension of police surveillance into the private domain of communications.

### **Identity Profiling**

Though government can state benign purposes for wanting to aggregate large quantities of personal data, such as informing next of kin in emergency situations, there are many more uses to which such data can be put that are not at all benign. One example that is relevant in the current, post 9/11 political climate is the potential use of such information for "identity profiling". The aggregation of large amounts of personal data is a prerequisite for government to engage in this controversial practice.

Governments, including Canada's, are increasingly using modern computer technology for purposes of data matching and data mining to construct profiles of those they think are likely to commit or to have committed crimes. They then take advantage of large pools of personal data to search for individuals who match the profiles. Not only do such programs subject the entire population to surveillance; they also make it feasible to target particular individuals on the basis that they share racial or cultural characteristics, or even political opinions.

CNA and LSPID are personal information. Although this information is often publicly available, it still carries some expectation of privacy. For example, many individuals choose to have unlisted telephone numbers.

Where it is not already publicly available, CNA and LSPID should only be available to law enforcement agencies upon judicial authorization once an appropriate threshold commensurate with the degree of privacy of this information has been met. Law enforcement agencies should not have access to this information prior to meeting that threshold.

- 11 -

The proposal for a national database should also be rejected on the grounds that it is unlikely to be effective or accurate, one reason being that the criminals police hope to identify will use false names and addresses. The proposal would only serve to create a database of law-abiding citizens. Other reasons it would be likely to fail are the libertarian culture of the Internet and the public's well-documented concerns over privacy and security on the Internet.

Recent furors in Canada over the so-called "big brother database" created and then dismantled by the Human Resources Development Agency, and the massive problems of the national gun registry program, provide strong indicators of the likely fate of a national database of subscriber information. Public resentment and resistance toward such a registration regime would almost certainly confound the effort.

### **DATA PRESERVATION ORDERS**

The federal government makes two proposals. The first is provision for "an expedited judicial order" that would require service providers to store and save existing specific data. The data would be preserved "only as long as it takes law enforcement agencies" to obtain a judicial warrant to seize or to produce the data. The purpose of the order would be to provide a "stop-gap" to preserve data that might otherwise be deleted. Secondly, the government proposes that in exigent circumstances, law enforcement agencies should be able to impose a preservation requirement on a service provider without a judicial order, for a specified period such as four days.

Preservation orders do not presently exist in Canada, and their creation would be an unprecedented and unjustified expansion of law enforcement powers.

Again, there is no statement in the Consultation Document justifying the need for these orders. There is nothing to suggest that law enforcement agencies are experiencing difficulties with the destruction or loss of data. Until there is this justification, these proposals should be rejected.

The Consultation Document asks whether a data preservation order should apply not only to stored computer data but to paper records as well. This proposal should also be rejected. The Consultation Document does not identify any problems that have been experienced with the destruction of paper records.

Preservation orders are an exceptional remedy. They should never be used for "fishing expeditions" or as a source or a pool of data that is available should law enforcement agencies ever suspect wrongdoing. If preservation orders are enacted, they must only be available with judicial authorization after an appropriate high threshold has been met, including reasonable and probable grounds to believe that the data sought will be destroyed, lost or modified. The Consultation Document does not set out what threshold is envisioned.



- 12 -

Further, there would have to be specific provisions to:

- prescribe the time limit for preservation orders;
- protect the confidentiality and security of the preserved data; and
- prohibit the disclosure of any of the preserved data unless and until a judicial order for production is obtained.

The time periods suggested by the Consultation Document are not justified. Preservation orders must not become a backdoor to circumvent the high thresholds and judicial authorization required for lawful access.

The government also proposes that in exigent circumstances, law enforcement agencies should be able to impose a preservation requirement on a service provider without a judicial order, for a specified shorter period. We reject such proposal for the foregoing reasons. Further, a preservation order is already "an expedited judicial order".

Finally, although data retention — the routine, longer-term retention of all electronic messages — is not being proposed, we are very concerned that data preservation is the first step towards such a result. Developments on data retention internationally, notably in the EU, may put pressure on Canada to enact such powers. The retention of vast amounts of information including clickstream traffic would be a major expansion in the ongoing assault on privacy.

## **INTERCEPTION OF E-MAIL**

The federal government seeks clarification with respect to the status of e-mail, and whether lawful access to it should be granted under the higher threshold for interception orders required for "private communications", or whether access should be granted under a lower standard required for search warrants.

There is a high expectation of privacy in e-mail and lawful access to it should be obtained only under the high standard for interception orders. E-mail is akin to a private oral communication. The Criminal Code should be amended to clarify that e-mail, whether in transit or in storage comes, can only be accessed under this higher threshold.

## **SUMMARY AND GENERAL CONCERNS REGARDING THE PROPOSALS**

Finally, it is important to view the proposals in the Consultation Document in the context of other legislation that is proposed or has recently been enacted. Privacy rights in Canada are continually under assault, and there has been a chipping away of these rights in the post 9/11 world. The recent anti-terrorist



- 13 -

legislation and Canada Customs and Revenue Agency's program to create a national database on people entering and leaving the country are two recent examples of this disturbing trend.

We must be vigilant to ensure that the right to privacy of Canadian citizens is only limited by such measures that are truly required, reasonable, demonstrably justified, effective and proportionate to the ends to be achieved. The proposals in the Consultation Document show clearly that these requirements have not been met.

We would welcome to the opportunity to comment further on the proposals once further information regarding the necessity of the proposals is provided, and draft legislation has been completed.

Yours Sincerely,

s.19(1)

[REDACTED]  
President  
BC Freedom of Information  
and Privacy Association

This submission has been endorsed by:

Commonwealth Centre for Electronic Governance  
[REDACTED] Executive Director

Friends of Freedom  
[REDACTED] National Coordinator

Muslim Canadian Federation and  
Council of the Muslim Community of Canada  
[REDACTED] Vice President

National Privacy Coalition  
[REDACTED] Chair

Pierlot, Paul

---

From: [REDACTED]  
Sent: 2002 Dec 16 5:19 PM s.19(1)  
To: la-al@justice.gc.ca  
Subject: Response to Lawful Access Consultation Paper



Cover ltr Dec 16 2002  
Lawful A...



Dec 16 2002 Lawful  
Access Fina...

Attached please find the joint submission of Aliant Telecom, BCE Inc., MTS Communications Inc. and SaskTel, providing comments on the government's consultation paper on lawful access.

A hard copy will follow by mail.

Sincerely,

[REDACTED]  
Regulatory Law  
Bell Canada  
Floor 6, 105 Hôtel-de-Ville  
Hull (Québec) J8X 4H7  
Telephone: (819) 773-5811  
Facsimile: (819) 778-3437



Aliant Telecom Inc.  
BCE Inc.  
MTS Communications Inc.  
Saskatchewan Telecommunications

16 December 2002

s.19(1)

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor  
284 Wellington St.  
Ottawa, Ontario  
K1A 0H8

BCE and Bell

To Whom It May Concern:

On behalf of Aliant Telecom Inc., BCE Inc., MTS Communications Inc. and Saskatchewan Telecommunications (the Companies), I am pleased to provide the attached comments respecting the Government's Consultation Paper on Lawful Access.

The Companies collectively provide the overwhelming majority of residential and business customer connections in Canada, and represent a broad range of communications service providers, comprising incumbent telephone companies, non-dominant interexchange carriers, competitive local exchange carriers, wireless carriers and Internet service providers.

The Companies appreciate this opportunity to provide written comments, at this preliminary stage, on the government's proposals for an updated legislative framework for lawful access in Canada.

The Companies believe that an ongoing, cooperative dialogue between law enforcement, industry and government is key to adequately addressing the complex questions raised by these lawful access proposals. The importance of this dialogue will become even more important as lawful access reform moves from the conceptual, to the legislative and regulation making stages, then on to implementation.

110 O'Connor  
Floor 14  
Ottawa, Ontario  
K1P 1H1

Tel: (613) 785-2180  
Fax: (613) 785-2182

- 2 -

The Companies look forward to future consultations, and the opportunity to make further submissions with respect to any legislation or regulations that may flow from the current proposals.

Yours truly,



s.19(1)

BCE and Bell

Attachment



**Customer Service in the Public Interest:**

**Response to Lawful Access Consultation Paper**

**of**

***Aliant Telecom Inc., BCE Inc., MTS Communications Inc.  
and Saskatchewan Telecommunications***

**December 2002**

## Customer Service in the Public Interest:

### Response to Lawful Access Consultation Paper

#### I. Introduction

Aliant Telecom, BCE Inc., MTS Communications Inc. and SaskTel (the Companies) are pleased to respond to the government's consultation document on lawful access, released 25 August 2002.

The Companies collectively provide the overwhelming majority of residential and business customer connections in Canada, and represent a broad range of communications service providers, comprising incumbent telephone companies, non-dominant interexchange carriers, competitive local exchange carriers (CLECs), wireless carriers and Internet service providers (ISPs).

The Companies recognize the need for law enforcement and national security agencies to have the necessary tools to protect private and national security interests, perhaps all the more so during these trying times, where threats relating to international terrorism are a pressing concern for all Canadians. The Companies have a long history of cooperation with the law enforcement and security community, and support lawful access to private communications by these groups, subject to appropriate legal process and judicial oversight.

At the same time, the Companies must carefully balance their own desire for good corporate citizenship, and the overarching societal interests in law enforcement and public safety, against the rights and expectations of their subscribers and the realities of their businesses.

The Companies are generally supportive of the legislative proposals contained in the government consultation paper; however, we have a number of serious concerns -- most significantly, the potential economic burden to telecommunications service providers and the uncertain role of industry in the fleshing out and implementation of the government's proposal. At the same time, the Companies are very pleased to see that the consultation paper does not contain a proposal for mandated general data retention -- a move that could be logistically and financially disastrous for telecommunications service providers.

## II. Background

### *Commitment to Law Enforcement*

As is well-known to the government and the law enforcement community, the Companies have been working with law enforcement and national security agencies for many years in order to facilitate timely and cost-effective implementation of lawful access by these agencies.

To this end, we have made, and continue to make, significant investments with respect to network infrastructure, personnel and process and procedures - all to be able to respond effectively to lawful access requests. Some of the Companies have dedicated teams, tasked solely with managing our ongoing relationships with law enforcement, including lawful access assistance and implementation and updates on technological development and network design. When faced with new services and technologies, the Companies have cooperated with law enforcement agencies (LEAs) and security interests to design, develop and provide effective and efficient solutions for lawful access.

The Companies believe that over and above the obvious private commercial interests in law enforcement and national security, all Canadian businesses have a broader societal obligation to assist LEAs in their authorized efforts to ensure public safety and security. However, given the significance of telecommunications in the detection and prosecution of offences against public order, telecommunications service providers seem to carry a disproportionate burden relating to lawful access than that shouldered by Canadian business generally. The capital and operational requirements imposed on telecommunications service providers in this regard go well beyond the norm. To date, the Companies, have been able to arrive at mutually satisfactory financial arrangements through negotiation with LEAs and security agencies, whereby we have generally been compensated for our reasonable costs of providing assistance with respect to lawful access.

The Companies are strongly of the view that the public interest would best be served if their current relationships with law enforcement and national security agencies - including cooperative development of access solutions and processes, and fair compensation for reasonable costs - were to continue under any updated legislative framework for lawful access.

### *Canadian Telecom Environment*

The Canadian telecommunications market is a particularly dynamic and challenging one at the present time. Telecommunications service providers are faced with intense competition in many areas, both domestic and international. Margins are growing thinner, and there is increasing pressure on revenues across all market sectors.

At the same time, technology is developing rapidly, and with it, customer demands and expectations for solutions and service delivery. To stay in the game, telecommunications service providers must respond to market developments and consumer demand, striving to deliver these new technologies and services. These emerging technologies frequently require capital-intensive network and service upgrades. Financing such upgrades can be difficult, given revenue pressures and the increasing demand of the capital markets in the wake of the bursting of the dot.com bubble and the insolvency of many players, including several high-profile failures of large telecommunications ventures.

Amidst this challenging operating environment, telecommunications companies are also key players in the government's Innovation Agenda, helping to build the knowledge-based economy that has been recognized by the government as one of the main economic engines of our nation through this century.

The Companies are extremely concerned about the potential negative impacts of the increased financial and operational burdens that may be placed on the telecommunications industry as a result of the government's lawful access proposals. If not properly designed and implemented, the lawful access proposals could significantly compromise the ability of the Canadian telecommunications industry to meet customer demand for new and innovative services and solutions, could negatively affect the financial health of individual telecommunications service providers, and could significantly retard the development of the online economy.

### III. A First Step to Legislative Reform

The Companies consider that the lawful access consultation paper is a comprehensive and helpful document that explains the government's motivation and intention in proposing legislative solutions for lawful access, as well as exploring some of the legal and practical issues associated with these proposals. However, the consultation paper outlines a high-level, conceptual framework only. No draft legislation has been made available, nor have any draft regulations, which the consultation paper suggests will contain technical and other standards or requirements for a service provider.

As is oft said, the devil may be in the details. As it stands, it is impossible for telecommunications service providers to determine with any certainty what the full requirements of the proposed lawful access legislation might be. Accordingly, it is also impossible to provide an accurate assessment of the implications of such legislation on the Companies, based solely on generalities.

That being said, the Companies note that the current consultation process nevertheless provides industry stakeholders with a valuable opportunity to provide initial input, at a preliminary stage of the legislative process, with respect to the development of an updated legal framework for lawful access in Canada. By necessity, the Companies



response to the government's legislative proposals will also take a fairly high-level approach, corresponding to the nature of the consultation paper itself.

The Companies wish to stress that it is absolutely imperative that they continue to have the opportunity for meaningful, studied input at each stage of the legislative process, as well as during implementation of the new regime. A formal process should allow for further consultation and input on draft legislation, perhaps through the parliamentary committee process. Similarly, industry must be fully involved in the design and implementation of the technical standards and requirements that may be mandated by regulation.

In fact, given the operational and technical complexities associated with standards development and process implementation, the Companies propose that a government/industry working group be established as an appropriate forum for ongoing discussion and resolution of such issues. Precedents for such an approach exist with respect to the standards for telecommunications equipment, as well as a host of operational issues associated with the implementation of competition in various sectors of the Canadian telecommunications market. Ideally, the working group would work on a consensus model, with occasional disputes being resolved by a designated government authority, such as Industry Canada.

#### IV. Guiding Principles

As noted above, the Companies are necessarily limited to responding to the government's updated framework for lawful access at a fairly abstract level. While the Companies will attempt to respond, to the best of their ability, to some of the particular questions posed by the government in the consultation paper, in order to frame the discussion, the Companies would first like to suggest that the development of a new legislative framework for lawful access should be guided by five key principles. The rationale for and implications of each principle are described in some detail below.

##### *1. Clarity, Consistency and Predictability*

As the consultation paper notes, it is crucial that service providers know what is required of them. Accordingly, it is vital that any legislated lawful access requirements, including any technical standards or requirements imposed by regulation, be as explicit as possible.

In addition, it is imperative that any legislative requirements be applied consistently and fairly to all service providers. As discussed above, telecommunications service providers currently operate in a dynamically competitive and challenging market environment. Any lawful access requirements or burdens must be applied consistently to avoid any distortions to the competitive market that could result from unequal application of responsibilities, particularly, but not exclusively, with respect to cost burdens and cost recovery.

## *2. Costs to Industry: Minimized, Fair, Recoverable*

Perhaps the single greatest concern for the Companies are the additional costs that they may incur under the government's proposals.

In the Companies' view, it is reasonable for a business, and therefore its customers, to pay for the costs of capabilities and features that benefit the customers of that business. However, where the capabilities and features in question benefit society at large, and are not remedial measures directed at some undesirable aspect of the service in question, it is submitted that such costs should generally be funded by the general body of taxpayers, as opposed to customers of that particular business. Otherwise, the customers of particular businesses may end up unfairly carrying a disproportionate cost burden to support a greater social good. This, the Companies submit, is the way that government-mandated spending has tended to operate.

Similarly, the Companies submit that telecommunications service providers, and indirectly their users, should not be called upon to fund infrastructure capability for lawful access, which benefits all Canadian citizens and businesses. Otherwise, telecommunications users end up being singled out for a hidden tax used to fund law enforcement activity and national security initiatives.

Despite this sound principle of funding of public benefits, should the government nevertheless determine that it is appropriate for telecommunications users to fund lawful access infrastructure on behalf the general population, the Companies submit that any mandated service provider investments should be focused, efficient, demonstrably necessary and recoverable from customers.

Any mandated service provider investments should be focused on products and services, and in geographical areas, where such investments are clearly warranted by criminal or terrorist use of those services, in those areas. Thresholds for expenditures on lawful access infrastructure must be absolutely clear, and high enough that they will not have a detrimental impact on innovation, service introduction or extension. Care must be taken to ensure that lawful access capability requirements do not create a windfall for manufacturers. Any updated legislative framework must ensure that all service providers, including those whose rates are regulated, will be able to recover the additional costs from customers.

Service providers should not be responsible under any legislative scheme for lawful access (infrastructure and operational assistance) respecting private line or wholesale services: these should be the clear responsibility (legal and financial) of end-user service providers.

Finally, the Companies submit that they should continue to be able to recover, on a negotiated basis, the reasonable costs of providing operational assistance to law enforcement and security agencies.

### 3. *Business As Usual*

The Companies submit that a key component of any lawful access regime is that the ongoing operational practices of telecommunications service providers should be impacted as little as possible. Aside from the requirement to provide lawful access capability, service providers should continue to be free to operate their businesses as they see fit.

Service providers should collect the data that they require for business purposes, and retain it only as long as they reasonably require for business purposes. Indeed, with respect to personal information about individual customers, the *Personal Information Protection and Electronic Documents Act*, and the OECD principles and privacy best practices on which it is based, require no less. Service providers should only be required to verify data to the extent that they feel it necessary to do so for business purposes. Operational processes, data collection and retention practices should be allowed to continue to reflect real business needs. Telecommunications service providers are not an arm of law enforcement, nor should they be transformed into one by legislative enactment.

This means that there should be no mandated collection of Customer Name and Address Information. Any data preservation or production regimes should apply exclusively to data that service providers produce, collect or retain for their own business purposes. Similarly, although it is not a part of the lawful access consultation paper proposal, the Companies are strongly of the view that there should be no general mandated retention of data outside of clearly identified targets pursuant to judicial authorization. Preservation and production orders should also apply only to data in the clear control of telecommunications service providers; not to user-managed data, even if resident on our facilities.

The Companies note that any significant deviation from the principle of "business as usual" could have a significant detrimental impact on the development of electronic commerce, online business applications, and IP communications in general. As the government has recognized,<sup>1</sup> a key impediment to realizing the full societal and economic potential of what used to be referred to as "the Information Highway" is the issue of user, and particularly consumer, trust. The Companies and the government have worked hard to foster this sense of trust for Internet and intranet users, through self regulatory initiatives and legislative action. These efforts could be wasted if the government were to enact legislation that caused telecommunications service providers, and particularly IP-based service providers, to collect or retain, in any significant way, user data not otherwise required for business purposes.

---

<sup>1</sup> See *The Canadian Electronic Commerce Strategy*, [http://e-com.ic.gc.ca/english/strat/doc/ecom\\_eng.pdf](http://e-com.ic.gc.ca/english/strat/doc/ecom_eng.pdf)

#### 4. *Aim for the Middle of the Road*

As acknowledged above, lawful access is an important tool for law enforcement, perhaps more so now than ever. Canadian law enforcement and security agencies should have all judicially-authorized tools necessary to protect Canada and Canadians from domestic and international threats to our safety, property and way of life. However, Canada is too small a player in the international arena to be able to afford to be a leader in the provision of lawful access. Given the lack of international market power and influence by Canadian telecommunications service providers, the costs associated with pursuing a Canadian model "showcase" of lawful access capability and procedure might only impair the global competitiveness of Canadian service providers. Canada should generally take a moderate approach to lawful access, in line with a majority of industrialized nations.

#### 5. *No Liability for Service Providers*

Finally, it must be a central tenet of any lawful access regime that telecommunications service providers, operating in good faith, should not be criminally or civilly liable for any act or omission thought to be mandated or prohibited by legislation or regulation. For example, no service provider should be liable for breach of privacy suits for compliance with a wiretap warrant found to be invalid for a procedural irregularity. No service provider should be criminally liable for failing to preserve data that was deleted by the user shortly after the preservation order was served.

The Companies note that a provision currently exists in the *Anti-Terrorism Act*, whereby organizations are exempt from liability for complying in good faith with certain provisions of that legislation.<sup>2</sup> The Companies submit that a similar approach should be taken here.

### V. Specific Responses to Issues Raised

#### **Infrastructure Capability**

##### *General Requirements*

It is entirely unclear to the Companies at this time what is intended by the phrases "general operational requirements" or "basic intercept capability", so it is not possible to comment meaningfully at this time, beyond addressing the framework. Yet, these are absolutely key to an impact assessment of the whole lawful access proposal.

---

<sup>2</sup> See, for example, subsection 83.08(2) of the Criminal Code, as amended by S.C. 2001, c. 41, which removes civil liability for an act or omission reasonably taken to comply with a provision relating to freezing of property owned or controlled by a terrorist group, or subsection 83.1(2), which removes criminal and civil liability with respect to mandated disclosures to the RCMP/CSIS of the existence of terrorist property or information about a transaction relating to such property.

Certainly, it is essential to define and describe in explicit detail the operational requirements describing intercept capability and the scope of the regulation-making authority and forbearance-granting power. Without commenting on the content of any of the obligations or powers, the Companies find this to be a reasonable general approach to a legislative framework.

As discussed above, it is imperative that service providers be fundamentally involved at all stages of the development and implementation of these definitions and standards.

### *Regulations*

Again, the Companies can only comment at this point on the framework for regulations. As the consultation paper says, "It is crucial that service providers know what is required of them". We agree emphatically.

As for the legislation, the design and implementation of the Regulations requires a full public process, preferably featuring oral components. As discussed above, the Companies feel that a cooperative government/industry working group, mandated with a clear legislative framework, would be the best forum for the establishment of the matters proposed to be set out in the regulations.

We believe that it is appropriate for the Regulations to set out technical and other standards, perhaps by reference to the output or standards developed by the working group.

With respect to the terms and conditions pertaining to the security of interceptions and the delivery of the product of interceptions, some of these, too, could be appropriate fodder for the working group. Any terms and conditions driven exclusively by security and secrecy obligations should be clear, and should avoid delving too far into mandating certain operational practices and processes of telecommunications service providers. For example, it is a legitimate requirement of a wiretap that the existence of the wiretap be unobvious, and for knowledge of the existence of the wiretap to be highly restricted; however, the Regulations should avoid setting numerical maximums of the number of personnel allowed to know about the wiretap, or to mandate how the physical existence of the wiretap be rendered unobvious. These latter questions depend largely on the processes, division of labour and expertise of the service provider, and these differences must be taken into account in each situation.

The Companies are particularly concerned about using regulations to set standards for "the competence, reliability and deployment of employees" beyond the requirement for security clearances at a designated level. The Companies are open to allowing law enforcement and security agencies to provide training to security and technical employees of the Companies, and have long-accepted the requirement for security clearances; however, the proposed Regulations should not go so far as to micromanage

the operational procedures and hiring requirements of telecommunications service providers, particularly given that in many cases, lawful access assistance may be only a small component of that employee's job. Service providers can also not be unduly limited in providing for personnel redundancy. The Companies note that, particularly with respect to our unionized business units, there could be significant industrial relations issues that would arise from extensive requirements relating to qualifications, background checks, etc.

With respect to operational assistance costs, the Companies would state emphatically that the legislative framework for lawful access should provide for fees to be paid to service providers for operational assistance. Several of the Companies have incurred significant personnel and overhead costs just to respond to lawful access requests, sometimes maintaining whole teams dedicated to the law enforcement liaison function. We should receive reasonable compensation for this. As the government is aware, a small but vocal minority of law enforcement agencies is of the view that service providers need not be paid for operational assistance. The Regulations - or preferably, the legislation itself - should be explicit that reasonable fees are payable for operational assistance.

As stated above, the costs of providing operational assistance, as well as associated research and development costs, should be recovered on a negotiated basis wherever possible. In the Companies submission, the burden of lawful access demands, size, scope, technologies and operational and organizational approaches of telecommunications service providers vary widely. It would be inappropriate to attempt to develop a fixed, tariff-like approach to recovery of operational assistance costs.

### *Forbearance*

Forbearance could be a useful mechanism for dealing with transitional periods, where no off-the-shelf solutions exist for new services or technology; however, forbearance must be used sparingly, and for short periods, in order to avoid the creation of "intercept safe havens" and any potential distortions of competitive markets.

The Companies are particularly concerned about the vagueness of the proposed forbearance regime. The Companies understand that under this proposal, the obligation to comply with some or all of the requirements of the lawful access legislation or regulations could be temporarily lifted for certain service providers. Although the consultation paper suggests forbearance as a means of avoiding the creation of "intercept safe havens", the Companies fear that forbearance may have exactly the opposite effect. Moreover, inappropriate application of forbearance could lead to a distressing irony: when criminal and terrorist activity migrates to forborne service providers and services, non-forborne service providers could well be left with expensive, fully-compliant state-of-the-art lawful access showcases that are unused, the lawful access targets having moved to forborne havens.

In addition, the Companies are concerned that they will not even be aware when competitors have been granted forbearance. The Companies understand, from discussions during some of the oral consultations held between government and industry stakeholders that grants of forbearance would not be made public. While this makes some sense, from the perspective of avoiding general public knowledge of where the "intercept safe havens" may be, it also denies similarly-situated telecommunications service providers (who may, perhaps, be quite knowledgeable about systems and hardware limitations of other providers in the same market sector) the opportunity to make submissions on the legitimacy of forbearance requests. This secrecy might also shield the information that a competitor may have the cost advantage of forbearance from infrastructure capability requirements.

Finally, the Companies note that under the forbearance proposal, the federal cabinet would delegate its authority jointly to the Solicitor General and the Minister of Industry, who would prepare administrative guidelines to govern their management of forbearance requests. Consistent with the Companies' submissions above, it is submitted that industry must be involved in the drafting of these administrative guidelines, particularly if they provide substantive guidelines for the granting of forbearance, in addition to procedural matters.

### *Compliance Mechanism*

The Companies are committed to full compliance with any legislative requirements, and will continue to cooperate with all levels of law enforcement.

The Companies submit that, for larger service providers, compliance could be measured through the ongoing liaison between affected service providers and law enforcement and security agencies. For smaller carriers, a law-enforcement-funded inspection mechanism might be useful, but it should be one that focuses on recommendations, moving to penalties only in the clearest cases of non-compliance. It may be appropriate for the Solicitor General to do this on behalf of the various law enforcement and security agencies. It would be inappropriate and likely unworkable if each agency was to conduct its own inspections.

The Companies believe that contempt of court provides an adequate disincentive for non-compliance with warrants, preservation or production orders, and the like. Summary conviction offences may be appropriate for consistent, blatant, and unjustified non-compliance with infrastructure capability requirements.

### *Intercept Capability Costs*



As discussed in greater detail above, the Companies are of the view that intercept capability costs should be funded out of general tax revenues, rather than by users of telecommunications services.

However, if the government is nonetheless inclined to impose some or all lawful access infrastructure costs on industry, any such costs should be minimized, fair and recoverable from customers.

As noted earlier, the Companies are operating in extremely competitive markets, in which there are already huge business-related demands for capital spending. At the same time, there is pressure from the capital markets to reduce such spending. In the result, financing new capital ventures from either operating revenues or the capital markets can be a challenge. Throwing any additional expenses into this environment will present challenges for all telecommunications service providers, all the more so for wireline and wireless providers, where the breadth of service areas and dispersion of intelligence in networks could lead to significant costs for lawful access infrastructure. In some cases, as with some dial-up Internet service providers, facilitating lawful access is as simple as providing a port to divert transmissions to a listening post; in others, expensive hardware and software loads are required. For wireless providers, lawful access infrastructure costs could be several times current annual capital budgets. For wireline providers, necessary software upgrades could be as much as \$ .5 million per switch.

As the proposal contemplates that mandated lawful access infrastructure investments by telecommunications service providers will be triggered by the introduction of new technologies and services, or when a "significant upgrade" is made to systems or networks, these additional cost requirements will become factors in determining when and if such services will be introduced. Particularly where the lawful access infrastructure costs are significant and the projected margins are already thin or non-existent, mandated service provider expenditures could kill or retard the introduction of new services, or the extension of services to underserved areas. For example, the business case for the expansion of broadband connectivity to some communities could be rendered negative by the addition of lawful access infrastructure costs. The addition of a new line feature to a wireless or wireline calling feature portfolio might be avoided if the introduction would require new software downloads for each switch in the network.

It is submitted that neither innovation, nor extension of service, should be sacrificed to provide lawful access, particularly when such sacrifice could be avoided by funding from general government revenues, as opposed to imposing a hidden "tax" on telecommunications users. Thresholds for expenditures on lawful access infrastructure must be absolutely clear, and high enough that they will not have a detrimental impact on innovation, service introduction or extension.

Given the stakes, it is important that any expenditure required of telecommunications common carriers should be minimized. Service provider investments should be focused



on products and services, and in geographical areas, where such investments are clearly warranted by criminal or terrorist use of those services, in those areas. It is the understanding of the Companies that this is how law enforcement currently funds the design and provision of lawful access infrastructure: the money goes where there is a significant and demonstrated need. Nothing more should be expected with respect to the expenditure of service provider funds. Care should be taken to avoid the indiscriminate roll-out of a showcase of expensive lawful access technologies to all areas and services, since such an approach might well result in the needless expenditure of significant amounts of capital.

Similarly, the Companies note the absence of the telecommunications equipment and software manufacturers from the lawful access consultation document, and indeed, largely from the consultation process. This seems a significant omission, given the important role that such manufacturers will play in the proposed scheme. The Companies are particularly concerned that the lawful access infrastructure proposals will create a windfall for these manufacturers. The proposal seems to assume that manufacturers will build whatever telecommunications service providers will need in order to comply with infrastructure requirements, and that the competitive marketplace will provide sufficient discipline on pricing to protect service providers.

There is a danger that some manufacturers may not offer only those enhancements and features that are required to meet lawful access requirements. Rather, there is a real possibility that the Companies will, through bundled equipment and software offerings, be required to purchase more than they need to comply with the legislation. Where lawful access capability is software based, the competitive market is also not always helpful in acting as a price restraint, since many service providers must purchase proprietary software linked to hardware investments that they have already made - there is really only one vendor to choose from. Finally, the Companies find it discriminatory that, with respect to compensation for assistance to law enforcement, telecommunications service providers are essentially held to recovering costs (and, with some law enforcement agencies, cannot even expect that), while manufacturers are not subject to any pricing restraints whatsoever in providing service providers with the equipment and software needed to provide lawful access capability.

At a minimum, any legislation should state explicitly that manufacturers must make available to telecommunications services providers the features necessary to provide the required access capability at a reasonable charge, or preferably, at cost. The Companies note that a similar approach was taken in the United States, where Section 106 of the *Communications Assistance for Law Enforcement Act of 1994* (CALEA), Pub. L. No. 103-414, 108 Stat. 4279, explicitly acknowledges the important role to be played by equipment manufacturers:

(b) COOPERATION- Subject to sections 104(e), 108(a), and 109 (b) and (d), a manufacturer of telecommunications transmission or switching equipment and a provider of telecommunications support services shall, on a reasonably timely basis and at a reasonable charge, make available to the telecommunications carriers using its equipment, facilities, or services such features or modifications as are necessary to permit such carriers to comply with the capability requirements

of section 103 and the capacity requirements identified by the Attorney General under section 104.

For service providers not subject to rate regulation, the challenge will be to recover lawful access infrastructure costs from subscribers in a manner that does not create churn. For service providers that are subject to price-cap regulation, such as the incumbent telephone companies, these costs can only be recoverable within the existing pricing constraint under the price cap formula if they are viewed as exogenous variables. For such carriers, lawful access infrastructure costs **must** be viewed as exogenous variables, otherwise these carriers, unlike their forborne competitors, would unfairly have to simply absorb the significant capital expenditures that may be required by the government's proposal. Moreover, it may be difficult to assign an appropriate value for this exogenous factor, absent the assistance of manufacturers. For this reason, the government should require manufacturers to separate out, through distinct line items, the costs of lawful access capabilities from other features and capabilities that may be included with equipment and software.

At the same time, service providers should not be required to incur the additional expense of developing lawful access capability with respect to services or technology where no vendor solutions are available, since the costs of such development work (as well as ongoing support, and eventual replacement) could be prohibitive. The Companies will continue to work with law enforcement and security agencies to develop lawful access solutions where none exist, but given the vagaries of the solutions that may be required, their associated costs, and the degree of funding provided by the agencies, there should be no legislative requirement for service providers to provide customized solutions.

Another way to minimize potential expenditures for telecommunications service providers is for law enforcement and security agencies to cooperate to a greater extent by agreeing on standardized procedures for warrant execution and standardized methodologies and technologies for signal delivery to "listening posts". In fact, it seems to the Companies that both private and public funds could also be saved by joint surveillance and shared listening posts between various agencies, wherever the law or nature of the investigation make this possible.

Another way in which costs to telecommunications service providers should be minimized is not to make service providers responsible for lawful access respecting services where they have no direct relationship with the end user.

It is absolutely essential that the thresholds that trigger infrastructure investments be explicit and not subject to interpretation or uncertainty. Not only should definitions of "new technologies and services" and "significant upgrade" be provided, clear examples should also be set out. Only services that provide a significantly novel functionality should be considered "new". Enhancements or variations on existing or previously available services or features should not be considered "new".

Technologies that do not require a fundamental retooling of equipment or networks should neither be considered "new", nor constitute "significant upgrades". Simple changes in speed, capacity or protocol should not trigger infrastructure capability requirements. For example, the addition of additional speed options for Internet access, or the introduction of public Internet access kiosks, both of which run on existing infrastructure, should neither be considered "new" nor "significant upgrades".

In no case should the introduction of a "new" service, including an extension of an existing serving area, trigger the installation of access capability backwards through older and established services and networks. The tail should not wag the dog. For example, the addition of a new router or piece of switching equipment may trigger a requirement to ensure that that piece of equipment is compliant with capability requirements; however, it should not trigger a requirement to revamp all routers or switches in the network to produce and forward a piece of data required to make the lawful access capability installed in the new equipment completely operational. To use an example from the transition to digital switching in telephony, the addition of a switch capable of providing calling line identification (CLID) should not have triggered (and indeed, did not do so) a requirement that all parts of the network be upgraded to be CLID-capable.

The Companies also note that some software-enabled lawful access capabilities require not only installation of the required software, but the purchase of a "right to use" (RTU) before certain features can be made fully operational. It is submitted that, in order to minimize costs, it should be sufficient for service providers to merely maintain the general software capability, acquiring any additional required permissions only when a request is received that would require the feature in question. This sort of standby capability should be sufficient, provided that it can be turned up within a reasonable period of time. A fuller and more technical exploration of RTUs and an associated reasonable turn up period could be another appropriate task for the government/industry working group recommended by the Companies.

## **Amendments to Criminal Code and other statutes**

### ***Production Orders***

The Companies generally support the concept of production orders, noting they are preferable to the more intrusive, operationally disruptive nature of search warrants. The Companies also note that in many cases, search warrants might be less successful. In this regard, data sought by a warrant could be located in numerous places throughout databases and networks, known only to the architects and operators of the network.

The Companies will comply fully with all valid, judicially-authorized orders, but need to be given realistic amount of time to comply with such orders. The amount of time required will vary, depending on several factors, including the scope of the request, the

nature of the data and the number of sources from which it must be retrieved and the means by which the data must be accessed (e.g. are there existing electronic search tools, or must a program be written?).

The Companies also generally support the use of a lower standard for the production of telecommunications associated data and customer name and address information. In the realm of telephony, some of the Companies have offered, or are currently awaiting regulatory approval for, a service that would provide a reverse directory functionality to law enforcement. As previously authorized by the Canadian Radio-television and Telecommunications Commission, customer name and address information (CNA) should be available to LEAs without warrant, unless non-published, on a fee for service basis. The Companies would again submit that only CNA that a service provider collects for business purposes should be available. There should be no legislated requirement to collect or verify CNA for law enforcement purposes.

The Companies also consider that it would be appropriate to extend the provision of the Criminal Code providing for warrants for the installation of Dialed Number Recorders (DNRs)<sup>3</sup> to other types of traffic data, with the important proviso that, like DNR data, the traffic data should reveal only the source, destination, time and duration of the transmission – the content of the communication should not be revealed, directly or indirectly. In this regard, the Companies note that in the Internet world, traffic data could well reveal content details, such as when viewing web pages on the Internet. Access to any such details should be subject to the higher standards for judicial authorization that are applicable to wiretaps.

Accordingly, the Companies recommend that the definition of “telecommunications associated data” provided in the consultation paper should be amended by adding, at the end of the definition, “that does not reveal, directly or indirectly, material details of the content of the transmission.”

### *Assistance Orders*

The Companies will comply fully with court orders, and have a long history of cooperation with law enforcement, including with respect to execution of warrants. The Companies expect this relationship to continue. In fact, we prefer to offer assistance to law enforcement in execution of warrants, since we know our own networks, practices and personnel better than law enforcement could.

Accordingly, the Companies do not consider assistance orders to be necessary. However, should the government determine that the power to make such orders should be included in the lawful access legislation, the Companies submit that the legislation should also specify that law enforcement should cover the reasonable costs of providing such assistance.

---

<sup>3</sup> Section 492.2.

### *Preservation Orders*

The Companies generally support the introduction of preservation orders into Canadian law, provided that such orders are explicit and unambiguous, narrowly targeted (both with respect to the subject and scope of data to be preserved), short in duration, and allow service providers a reasonable time to comply. As noted with respect to production orders, data may be stored in a variety of decentralized places, and time may be required to implement an order to preserve it.

The Companies are also generally comfortable with the concept of "exigent circumstances" preservation orders, without judicial authorization, provided that the data is required to be preserved for a very limited time – just long enough to obtain a court order. The Companies suggest that two working days should be sufficient. The Companies submit that each "exigent" request should be fully documented by the requesting law enforcement agency, and followed up with letter confirming it. There should be an explicit limitation of liability for service providers in responding to "exigent circumstances" preservation orders.

The Companies submit that it would be illogical to limit preservation orders by reference to a particular format or technology. Such orders would be appropriate for all forms of documentary and electronic information (including paper, fiche, source code, etc.), but shouldn't apply to data in the control of the end-user (such as voice mailboxes and user-posted data). Since these latter features were deliberately designed as user-controlled, they would be extremely difficult to preserve, while maintaining invisibility with respect to the user.

A simple "reasonable and probable grounds" standard may be appropriate for obtaining the requisite judicial approval, particularly if the duration for such an order is fairly limited, for example, 90 days.

As mentioned earlier, the Companies are of the view that contempt of court provides a sufficient disincentive for non-compliance with warrants and other court orders.

### *Virus Dissemination*

Viruses are a scourge to operators of corporate networks, as well as to Internet service providers. The Companies certainly support measures intended to reduce the number of viruses in circulation.

Accordingly, it may be appropriate to criminalize the creation, sale and possession of devices or programs intended to commit offences specified in the Convention on Cyber-

Crime. At the same time, such an offence must include a clear exception for the creation, sale and possession of legitimate self-assessment tools (such as various programs intended to test intrusion detection). The device or program in question must have been created, used or disclosed for the clear purpose of causing harm or mischief to third parties, whether or not unknown.

Again, it is extremely important, if new or expanded criminal liability for virus dissemination or storage is created to exclude from liability any service providers acting solely as common carriers either for transmission or hosting, if the service providers have no actual knowledge of the existence of the viruses.

### *Interception of eMail*

The Companies consider that the key to determining the appropriate treatment, from a lawful access perspective, of eMail and similar text-based electronic communications lies in whether or not the message has been received (i.e. read, viewed) by the intended recipient. The term "intercept" itself, suggests interference between the place of origination and the place of destination of the communication. Indeed, this appears to have been the approach taken by the courts with respect to the Invasion of Privacy provisions of the Criminal Code: *R. v. McQueen* (1975), 25 C.C.C. (2d) 262 (Alta. S.C.), *R. v. Singh* (1998), 127 C.C.C. (3d) 429 (B.C.C.A.).

If the message has not been received (i.e. unopened, unreceived, unsent, etc.), it should be viewed as being in transit, and be considered to be a "private communication," within the meaning of s. 183 of the Criminal Code, and subject to lawful access using the standard applicable to wire taps under s. 186. This would include data associated with the composition of messages (keyboarding), transmission, and holding or storage before receipt or viewing by a service provider or intermediary, or incidental holding or storage by such a provider. The Companies consider that there is a reasonable expectation of privacy by the users of eMail, chat, SMS messages, and the like, given the two-way, ephemeral nature of the communication. The Companies would support a broadening of the definition of "private communication" to explicitly capture these other forms of traffic, if such an amendment is considered to be necessary.

By contrast, the Companies believe that there is an inherently lesser expectation of privacy with respect to stored material, since it is available for viewing by and distribution to others. The Companies are also of the view that this lesser exceptional of privacy also applies to stored materially incidentally kept by telecommunications service providers. Once viewed or read, a text message becomes more akin to a stored document if the user decides to retain (save, leave in inbox, etc.) the document. Accordingly, a search warrant or production order should be required for law enforcement to obtain lawful access to such communications.

The Companies believe that the Criminal Code should be amended to explicitly recognize these two "streams" of electronic text messaging, associating them with the lawful access orders and authorization standards discussed above.

### *Competition Act Amendments*

The Companies have little to add with respect to the proposed amendments to the Competition Act. We generally support judicially-authorized access by the Competition Commissioner to hidden records, and the availability of assistance and production orders on the same terms and subject to the same safeguards as in the Criminal Code.

### *Other subscriber and SP information*

In the Companies' view, LSPID, CNA, and reverse search data should all be available to LEAs with respect to published numbers, without warrant and for a reasonable, negotiated fee. The Companies submit that there is a minimal expectation of privacy with respect to such data, and that privacy rights would not be seriously compromised by effectively prohibiting fully anonymous use (at least to law enforcement) of telecommunication services.

As noted earlier, access should be available only with respect to records kept by service providers for their own business reasons. There should be no requirements to retain such data just in case it might be needed by law enforcement. There should also be no obligation to verify the accuracy of any CNA data collected.

The Companies oppose the development of a national super database for CNA information. The Companies feel that their own databases are adequate for this purpose, and a new national database would add unexpected and unnecessary costs to what already looks like an expensive legislative proposal.

If the government is nevertheless inclined to mandate a national database, the Companies believe that the costs of such a database's establishment and maintenance should be entirely borne by the government. It may be appropriate that such a database be administered by a third party under contract (as was the case for telephone numbering and the Canadian telecommunications contribution fund).

With respect to the possibility of using 911 databases to obtain accurate and current information for law enforcement, the Companies submit that such a use would be inappropriate. The 911 database was created for emergency medical, fire and law enforcement assistance only. It contains precise geographic locations as well as street addresses (in some cases, especially assigned for the purpose of supporting 911 Service), and contains information over which individuals have little control or option. The 911 database should not be available for investigation purposes without warrant.

### *Conclusion*

The Companies appreciate this opportunity to provide comments on the government's proposals for a legislative framework for lawful access in Canada. The Companies also appreciate the opportunities that many of the Companies had to meet in person with various government stakeholders to better understand the government proposal and its implications.

The Companies believe that an ongoing, cooperative dialogue between law enforcement, industry and government is key to adequately addressing the complex questions raised by these lawful access proposals. The importance of this dialogue will become even more important as lawful access reform moves from the conceptual, to the legislative and regulation making stages, then on to implementation.

The Companies look forward to future consultations, and the opportunity for industry stakeholders to make further submissions at the legislative, regulation-making and standards-setting phases.



Pierlot, Paul

From: [REDACTED] s.19(1)  
Sent: 2002 Dec 16 6:00 PM  
To: la-al@justice.gc.ca  
Subject: Lawful Access - Consultation Document

I'd like to submit a couple comments about the proposed amendments to the Lawful Access provisions. My tenure in the Internet-related industry in Canada has spanned 7 years and as a developer and administrator

My main contention is with the section on 'Virus Dissemination'. It states in part:

A minor change in the wording of section 342.2 would be necessary to clarify that the creation, sale and possession of a computer virus program for the purpose of committing a computer offence or mischief is an offence in Canadian law.

Firstly, the reliance on the term 'Computer Virus' here either demonstrates a lack of familiarity with the variety of program types available for attacking computer systems, or the intention to use this single term to describe all programs that may be used to attack a computer system. In either case, this has to be clarified, the term 'Computer Virus' defines a specific kind of computer program which may be used to attack computer systems, Canada should strive to not dilute it's definition with such generalizations.

Secondly, the possession of such tools, whether it be a Computer Virus specifically or any other program used to attack a computer system, should not be considered a crime. Even if it is guarded with a 'malicious intention' clause, as above, the use of such tools is actually a valuable boon to professionals in the IT industry who need to evaluate a computer system's performance and security. To place these professionals in a position where they may have to defend their thoughts and intentions, without having launched an attack or even properly conspired to do so, would do damage to the IT industry and it's defense mechanisms to online threats.

Thank you for the opportunity to voice my opinion on the matter of these proposed amendments, had I known about this earlier I would've had the time to contribute more comments.



Pierlot, Paul

---

From: Regulatory Matters [Regulatory.Matters@TELUS.COM]  
Sent: 2002 Dec 16 6:10 PM  
To: 'la-al@justice.gc.ca'  
Subject: Lawful Access - Consultation Document



telus\_161202.zip

Type of Filing: Submission

Title/Subject: TELUS Submission to the Lawful Access - Consultation Document

Filing Date: December 16, 2002 - Company Name: : TELUS Communications Inc.

Description: Submission of TELUS in response to the Government of Canada's call for comments on the Lawful Access - Consultation Document

List of filenames: telus\_161202.zip

<<telus\_161202.zip>>



TELUS  
31 - 10020 100 Street NW  
Edmonton, Alberta  
Canada T5J 0N5

telus.com

[Redacted]  
Vice-President  
Public Policy & Regulatory Affairs

s.19(1)

(780) 493-6590 Telephone  
(780) 493-6519 Facsimile  
[Redacted]

December 16, 2002

Lawful Access Consultation,  
Criminal Law Policy Section  
5<sup>th</sup> Floor,  
284 Wellington St.,  
Ottawa, Ontario,  
Canada, K1A 0H8.

Dear Mr. Paul Pierlot:

**RE: TELUS Submission to the LAWFUL ACCESS – CONSULTATION  
DOCUMENT**

Enclosed please find the submission of TELUS Communications Inc. ("TELUS") on behalf of itself and its affiliates, TELUS Quebec and TELUS Mobility in response to the Government of Canada's call for comments on the **LAWFUL ACCESS – CONSULTATION DOCUMENT** issued by the Department of Justice, Industry Canada and the Solicitor General Canada on August 25, 2002. A copy of these comments has been filed by email to [la-al@justice.gc.ca](mailto:la-al@justice.gc.ca).

Yours truly,

*{original signed by* [Redacted]

[Redacted]  
Vice-President  
Public Policy & Regulatory Affairs

PD/pk

Encl.

**SUBMISSION OF COMMENTS  
BY  
TELUS COMMUNICATIONS INC.**



**December 16, 2002**

**to the**

**GOVERNMENT OF CANADA**

**on the**

**LAWFUL ACCESS CONSULTATION DOCUMENT**

**Department of Justice  
Industry Canada  
Solicitor General Canada**

**Issued August 25, 2002**

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	1
COMMENTS BY TELUS.....	5
"HARMONIZATION", NOT A "MADE IN CANADA" APPROACH, IS ESSENTIAL.....	6
NEED FOR REASONABLE TRANSITION PERIOD, FORBEARANCE AND GOVERNMENT FUNDING.....	7
LIMITATION OF LIABILITY PROVISIONS AND CHARTER PROTECTIONS .....	8
LAWFUL ACCESS ISSUES RAISED IN THE CONSULTATION DOCUMENT .....	8
SCOPE OF THE TELUS COMMENTS .....	9
MORE PUBLIC CONSULTATION IS REQUIRED .....	10
LACK OF LAWFUL ACCESS EQUIPMENT REQUIREMENTS, NOT NEW COMPETITORS AND NEW TECHNOLOGY, MAKE LAWFUL ACCESS DIFFICULT .....	11
LAWFUL ACCESS SHOULD BE COMPETITIVELY NEUTRAL.....	12
LAWFUL ACCESS SERVICES SHOULD BE PAID BY THE FEDERAL GOVERNMENT OR BY LEAS .....	15
PRICES FOR SERVICES SHOULD BE DETERMINED BETWEEN THE "BUYER"( THE LEA) AND THE "SELLER" ( THE SERVICE PROVIDER).....	17
THE AMBIT OF THE PROPOSED LEGISLATION .....	18
THE LAWFUL ACCESS PROPOSALS RISK BEING IN CONFLICT WITH THE GOVERNMENT'S INNOVATION STRATEGY. ....	19
NEED TO REDUCE RISK AND UNCERTAINTY BY DEFINING TERMS IN A GOVERNMENT/INDUSTRY WORKING GROUP .....	20
TELUS PROPOSES REGULATION BY REFERENCE AS BEING A FASTER, MORE FLEXIBLE MODE OF OPERATIONS .....	21
POINT OF DEMARCATION / END OF SERVICE PROVIDER RESPONSIBILITY .....	22
STATUS QUO FOR SERVICE PROVIDER PERSONNEL QUALIFICATIONS .....	22

FORBEARANCE IS A NECESSARY TOOL LEADING TOWARDS LAWFUL ACCESS REQUIREMENTS.....	23
THE REQUIREMENT FOR NEW LAW ENFORCEMENT TOOLS .....	25
IDENTIFICATION OF LOCAL SERVICE PROVIDER AND CUSTOMER REVERSE DIRECTORY SERVICE .....	28
SET-UP OF A REVERSE DIRECTORY: TELEPHONE NUMBER = NAME AND ADDRESS .....	29
OPPOSITION TO COLLECTION OF PERSONAL SUBSCRIBER DATA UNNECESSARY FOR SERVICE PROVISION .....	30
WHICH ADDRESS IS IMPORTANT IN CUSTOMER NAME AND ADDRESS? .....	31
A DISTRIBUTED SERVICE PROVIDER CNA DATABASE WITH NATIONAL COORDINATION MAKES MOST SENSE .....	31
CNA NATIONAL COORDINATION IS BEST LEFT TO OPERATION BY A THIRD PARTY INDUSTRY CONSORTIUM.....	32
CONCLUSIONS AND RECOMMENDATIONS.....	34

## Executive Summary

1. TELUS appreciates the opportunity to submit comments on the Government of Canada's *LAWFUL ACCESS CONSULTATION DOCUMENT* (the "Consultation Document") issued by the Department of Justice, Industry Canada and the Solicitor General Canada on August 25, 2002. TELUS is also pleased that Justice Canada extended the deadline as requested to December 15, 2002 to allow more substantive comments to be provided on this important issue.
2. TELUS has a long history of cooperating with law enforcement authorities and aiding them to carry out their lawful mandate as provided for by Parliament. TELUS recognizes that lawful access is an essential tool for national security and law enforcement and understands the motivations driving this initiative to update law enforcement tools. In supporting the Federal Government's initiatives in lawful access, TELUS assumes that all the necessary provisions of due process under the Charter would apply to these proposed activities. TELUS is also supportive of legislation that would provide a clear and transparent framework setting out the terms under which service providers are to provide assistance for lawful access.
3. As an overarching comment, TELUS suggests that further, more detailed consultations are required and recommends that Justice Canada release a draft bill and its associated regulations for public comment and input prior to proceeding to Parliament for First Reading. As a second overarching comment, TELUS requests that the Federal Government provide limitation of liability provisions in this new regime so that if a service provider, acting in good faith, inadvertently violated the privacy and confidentiality of a customer in response to a law enforcement request, no liability would ensue.

4. TELUS has reviewed the Consultation Document carefully and identified four principal issues where it seeks public input. These are:
  - lack of intercept capability (in existing telecommunications equipment or in equipment providing new-technology services)
  - casual use (anonymous) telecommunications services where requiring positive, verifiable identification of the users would dramatically change the operating parameters of the services
  - the need for a current and up-to-date telecommunications services database listing subscribers
  - development of new tools for interception and modification or enhancement of existing tools
5. In response, TELUS has prepared extensive comments on the first three points listed above. With respect to the fourth point, TELUS assumes that the Federal Government and civil liberties groups will deal adequately to set up new and revised law enforcement tools, and conditions of use, that are consistent with the Charter.
6. TELUS understands that many foreign governments are now reviewing and updating their lawful access tools. For this reason, TELUS urges the Federal Government to harmonize its lawful intercept requirements, particularly with those in the U.S., to help reduce the costs of provisioning and ensure that Canadian industry is not disadvantaged competitively by unique "made in Canada" requirements.
7. During the consultation process, TELUS has been troubled with the imprecise definitions of several terms including "forbearance" and "significantly upgraded service" and notes the need for precision as a prerequisite for understanding.
8. TELUS recommends in its submission that sufficient federal funding be made available to service providers to:



- retrofit all networks and systems
  - pay service providers for their operational costs
  - cover all incremental costs to provide the capability for lawful access to new networks and systems providing upgraded, significantly enhanced and new services
9. While it appears that there is a consensus on the first two points, the Federal Government does not currently propose to cover lawful access costs associated with the provision of new and significantly upgraded services. That can be a serious problem if, in failing to fully fund all costs associated with its lawful access agenda, the Federal Government decides to simply foist part of those costs onto only a few select players in the telecommunications industry. Such action could seriously distort the operation of market forces and competition.
10. TELUS is also concerned about ensuring the integrity of the lawful access regime. While it appears that consideration is being given to offering forbearance or even exemption for certain smaller service providers, largely based on the acknowledged impact of the costs of compliance, TELUS notes that if compliance costs are covered, these concerns largely disappear. In our view, covering all costs for the lawful access regime seems to be the only way to reduce or eliminate the safe havens that might otherwise be created with exemption and extended forbearance. Wherever forbearance is proposed, TELUS recommends that requests be assessed by Industry Canada and the Solicitor General jointly as per the successful model that has been in use for the past six years among the holders of PCS licences.
11. In an associated matter, TELUS is a contributor to the Government's Innovation Strategy. TELUS is concerned that these Lawful Access proposals set up impediments to innovation by requiring Canadian service providers to pay the costs for lawful access whenever they provide new and significantly upgraded services. TELUS recommends that the desire to provide new services to Canadians that also satisfy the needs of law enforcement be reconciled in such a

way as to maintain the innovative nature of our economy, as well as the individual's rights to privacy.

12. The ISP industry in Canada is composed of a large number of relatively small firms competing for subscribers. ISPs act like railways to connect users to information while at the same time (in the railway analogy) they also provide information sidings where information awaits pick up or further forwarding by users. Similar to the case with earlier federal legislation, companies are concerned with the prospect of having to defend against a zealous prosecutor who may have found viruses on an ISP's information siding or server. ISPs are comforted to know that they would probably be found not guilty for reasons of having neither knowledge of the viruses nor criminal intent, but the time, resources and effort required to defend could be debilitating to the company. For this reason, TELUS recommends that:

- there be no onus on ISPs to search out what's stored on their servers to ensure that they are "clean" of viruses; and
- an ISP should not attract liability if one of its subscribers stored a computer virus on its server
- any legislation or regulations make this explicitly clear

13. TELUS has serious concerns about the process of collecting, maintaining and accessing databases of service provider customer information. If it is determined that a Customer Name and Address (CNA) database is required, TELUS considers that access to such a database for law enforcement purposes should be operated by an independent third party, separate from both law enforcement and service providers. TELUS recommends study of three industry consortium companies (LNP, CPCC and CNAC) as possible models for the establishment and operation of a "front-end" system, administered by a neutral third party operator, for law enforcement to access customer name and address information under specified controls.

14. TELUS suggests that the independent third party operate a "front-end" coordinating role to take law enforcement requests and court orders where necessary and access service provider databases to obtain the information. Service provider databases would remain separate. This will ensure the protection of sensitive customer lists between service provider competitors and, at the same time, ensure that the proper Charter protections are submitted by law enforcement before information is provided.
15. TELUS also objects strongly to the imposition of any obligation that would require us to collect, maintain or guarantee the accuracy of CNA information if we have no corporate need to do so.
16. There are always questions about the degree of detail and specificity that may be included in legislation and regulations that will be applied rapidly in the fast changing, high tech world of telecommunications. TELUS sees the need for a flexible regulatory regime. No matter what regime is eventually imposed, there will still be implementation issues that will require substantive, ongoing discussion and cooperation between law enforcement and industry. TELUS recommends that the Federal Government convene a group with industry to work on such implementation guidelines. TELUS would welcome the opportunity to contribute to such a group.

#### COMMENTS BY TELUS

17. The following comments with respect to the LAWFUL ACCESS CONSULTATION DOCUMENT (the Consultation Document) dated 25 Aug 2002 are submitted on behalf of TELUS Communications Inc. and its affiliates, including TELE-MOBILE COMPANY (doing business as TELUS Mobility) and TELUS Quebec (collectively, "TELUS"). Failure by TELUS to address any specific aspect of this Consultation Document should not be construed as

acceptance or approval of the proposals as presented where such acceptance would be inconsistent with the Company's interests.

18. As a first comment, TELUS Communications Inc. is a member of the Canadian Association of Internet Providers (CAIP) and the Information Technology Association of Canada (ITAC), and its affiliate, TELUS Mobility, is a member of the Canadian Wireless Telecommunications Association (CWTA). TELUS was supportive of the requests by ITAC, CAIP and CWTA to Justice Canada for an extension to the comment period, which was specified initially, to close on November 15, 2002. TELUS is pleased that Justice Canada extended the deadline as requested, to December 15, 2002 to allow for more substantive comments to be provided on this important issue and to allow for additional meetings.
19. TELUS has a long history of cooperating with law enforcement authorities and in aiding them to carry out their lawful mandate. TELUS recognizes that lawful access is an essential tool for national security and law enforcement and recognizes the challenges faced by Canada's law enforcement agencies (LEAs) in carrying out their mandate in an increasingly complex technological environment. TELUS also understands the Federal Government's desire to create a clear and transparent framework under which service providers are to provide assistance for lawful access.

**"Harmonization", Not A "Made In Canada" Approach, Is Essential**

20. The move to establish a set of lawful access requirements in Canada is similar to other initiatives taken by law enforcement in a number of other countries faced with these needs, notably the G8. This lawful interception development work is underway simultaneously and will deal with the same types of telecommunications services provided by the same generic types of telecommunications equipment.

21. *TELUS urges the Federal Government to harmonize its requirements with those in other countries, particularly with those in the U.S. to help reduce the costs of provisioning and to ensure that Canadian industry is not disadvantaged competitively by unique "made in Canada" requirements.*

**Need For Reasonable Transition Period, Forbearance And Government Funding**

22. It is clearly the Federal Government's duty to protect its citizens from crime and national security threats. These lawful access proposals are being advanced by the Federal Government for the benefit of all Canadians. The Government, and ultimately the public at large, should pay the cost of implementing these proposals out of general tax revenues, as is the case with other policing and national security costs. It would be unacceptable for the Federal Government to shift the burden of the cost of implementing its lawful access proposals on to the shareholders or customers of service providers, as all businesses and citizens are the beneficiaries.
23. *TELUS therefore recommends that sufficient federal funding be made available to service providers:*
- *to retrofit all networks and systems to satisfy all lawful access needs of LEAs;*
  - *to cover all incremental costs to provide the capability for lawful access to new networks and systems providing upgraded, significantly enhanced and new services; and*
  - *to pay service providers, as necessary, for their operational costs to provide all lawful access services that may be requested by local, regional and national law enforcement authorities.*
24. When these lawful access requirements are eventually developed and adopted, TELUS urges Government to provide both a transition period and the financial resources to retrofit them into the Canadian telecommunications network. During a transition period after the lawful access needs are clearly defined but before they can be fully enforced, TELUS supports the proposal to offer a period of

forbearance to allow timely service deployment. Similarly, if these lawful access needs are modified in future to meet new and unforeseen government requirements, TELUS recommends that the government provide time and resources for a phased-in implementation. Finally, when new or significantly enhanced telecommunications services are created, TELUS expects that the government will support the innovation and productivity improvements afforded by the enhancements by contributing fully to all incremental lawful access costs that ensue.

### **Limitation Of Liability Provisions and Charter Protections**

25. TELUS requests that the government provide limitation of liability provisions in this new regime so that if a service provider, acting in good faith, inadvertently violates the privacy and confidentiality of a customer in response to a law enforcement request, no liability would ensue. TELUS assumes that appropriate Charter protections would apply to all of these activities.

### **Lawful Access Issues Raised In The Consultation Document**

26. TELUS has reviewed the document carefully and identified that there are four main issues on which the Consultation Document seeks public input. These are:
1. lack of intercept capability (in existing telecommunications equipment or in equipment providing new-technology services) and the need to rectify that inadequacy;
  2. casual use (anonymous) telecommunications services where requiring positive, verifiable identification of the users would change the operating parameters of the services;
  3. a current and up-to-date telecommunications services database listing subscribers' names and addresses plus the service provider, phone number(s) for each service;
  4. modified and new tools in the way of interception and search warrants to enable law enforcement to respond to new challenges.

## Scope of the TELUS Comments

27. In response to the law enforcement issues raised above, TELUS has prepared comments on the first three issues. With respect to the fourth issue, TELUS assumes that the Federal Government will be able to establish an appropriate balance between the need to set up new and revised law enforcement tools on the one hand and the rights of the individuals whose information will be collected on the other.
28. TELUS was mindful of the following principles as it reviewed the proposals in the Consultation Document:
1. the requirement to respond to lawful access requests by law enforcement;
  2. the need for funding for both the capital costs and the operational costs of enabling the network to meet the needs of lawful access as they are eventually approved in legislation and regulations;
  3. the need for competitive neutrality in the implementation of this lawful access regime so that all service providers share an equitable responsibility;
  4. the need for transparency in implementation of lawful access so that it does not change the way telecommunications services can be provided to Canadians;
  5. the need for harmonization of lawful access requirements in Canada vis à vis those in our major trading partners so that Canadian telecommunications consumers and service providers will not have to shoulder special "made in Canada" burdens not required elsewhere and telecommunications equipment suppliers will not have to design Canada-only "extras";
  6. the need to restrict lawful access requirements to those provisions that are technically feasible, cost-justified and are effective in meeting law enforcement and national security needs.
29. With these important principles in mind, TELUS will respond to the Consultation Document and its issues and questions.

## More Public Consultation Is Required

30. Early in the Discussion Paper, there are references to the Council of Europe Convention on Cyber-Crime and its work over the past years where Canada was a permanent observer. The Consultation Document notifies Canadians that Canada along with 33 other countries signed this Convention calling for the criminalization of certain activities, mutual legal assistance and extradition provisions, all dealing with computer systems and telecommunications networks. Justice Canada has a long and respected history of consultation on many issues that matter to Canadians from provisions relating to young offenders, to those dealing with gun registration. However, in this case, TELUS has concerns about the lack of transparency with respect to the previous negotiations relating to The Council of Europe Convention on Cyber-Crime. Canadians now appear to be faced with a "fait accompli."
31. In TELUS' view, this lack of transparency surrounding the negotiations is unfortunate. In future, TELUS suggests that any such contemplated measures that will affect the telecommunications industry and its users be brought to public attention and that public input be solicited much earlier in the process.
32. The topics raised in this consultation require a review that is an extremely complex undertaking, involving several acts of Parliament (*Criminal Code*, *Radiocommunication Act*, *Competition Act*, *Personal Information Protection and Electronic Documents Act*, etc.) It will require implementation by law enforcement staff at three levels of government (police at federal, provincial and local levels) and require new regulations and perhaps working guidelines to be successfully implemented. TELUS finds it difficult to comment on the proposals stated in this Consultation Document without having an appreciation for the whole picture. In TELUS' view, it would have been preferable for the Federal Government to have released this Consultation Document, along with a draft bill



and the underlying regulations, to allow a fulsome dialogue between industry and government. The consultation document outlines, only in very general terms, what is contemplated in implementing the Cyber-Crime Convention. Without a draft bill and proposed regulations to refer to, TELUS is unable to see how all the pieces of the puzzle are going to come together to form an effective lawful access regime that will govern our relationship with law enforcement. In TELUS' view, industry needs to be given an opportunity to comment on the draft legislation, regulations and guidelines to see how the various elements will all work together, prior to their enactment.

33. For this reason, comments provided by TELUS in this submission are without prejudice to comments, which may be developed after the legislation is introduced. Hopefully, draft regulations will be made available to explain in some detail the regime that is being created.
34. *TELUS recommends that Justice Canada release a draft bill and its associated regulations for public comment and input prior to proceeding to Parliament for first reading of a Bill.*

#### **Lack Of Lawful Access Equipment Requirements, Not New Competitors And New Technology, Make Lawful Access Difficult**

35. As a general comment, TELUS notes the references in the Consultation Document to the rapidly evolving environment in the telecommunications and Internet industry where competition has replaced monopoly provision of local, long distance, overseas and wireless services. In addition, the Consultation Document also notes the advent of new electronic storage and communications technologies and devices to exploit them. According to the Consultation Document, both have caused major difficulties in the ability of law enforcement authorities to carry out their lawful access activities.

36. TELUS does not believe that competition in telecommunication or the advance of technology has caused any difficulty to law enforcement. TELUS remains committed to the competitive development of Canada's telecommunications sector and to the deployment of new and innovative technologies, services, and devices. We see no conflict between that objective and the need for lawful access if the needs for lawful access are clearly described and become incorporated in equipment and service design specifications at the beginning of the design cycle.
37. *TELUS recommends that lawful access capabilities be required in all new equipment being considered for introduction to the Canadian telecommunications market place, which will be used for the provision of voice or data services.*

#### **Lawful Access Should Be Competitively Neutral**

38. The Consultation Document states that:

"It is essential to ensure that no competitive disadvantages are placed on Canadian industry and that the solutions adopted do not place an unreasonable burden on the public"

39. In ensuring that no competitive disadvantages are placed on Canadian industry, it is instructive to see the implementation of similar provisions in the US where the Communications Assistance to Law Enforcement Authorities (CALEA) Act appropriated \$500M (U.S.) for implementation, primarily for retrofitting the existing system, to cover the costs for service providers to install the necessary hardware and software to make their circuit switched voice networks meet the specified lawful intercept standards. This amount, we understand, was not sufficient to cover all reasonably incurred costs for retrofitting American networks.

40. In Canada, the Solicitor General has established equivalent standards<sup>1</sup> for lawful intercept as are contained in the US CALEA legislation. From a TELUS overview of the Canadian telecommunications sector, we estimate that it will cost approximately \$125 - \$150M to retrofit the networks and systems of Canadian carriers (local exchange carriers, inter-exchange carriers, wireless service providers and resellers) to bring them into compliance with the Solicitor General's standards. In order to ensure that "no competitive disadvantages are placed on Canadian industry", TELUS urges government to ensure that public funds be made available to pay all costs including those both to retrofit the existing network and those needed to outfit the network to provide new or significantly enhanced services.
41. It should be noted that these current Solicitor General Standards (and the equivalent CALEA Standards) address interception of circuit switched communications and are not easily "stretched" to address interception of packet transmissions, nor do they address data-preservation, interception of e-mail or the development and operation of a national subscriber database. If these lawful access initiatives are implemented as proposed, then technical/equipment standards have still to be developed with industry, and costs have to be paid to retrofit existing operations and to outfit the new systems with the lawful access capabilities required for the provision of new services to provide lawful access. TELUS notes that costs for these initiatives are in addition to the estimates of \$125M - \$150M estimated above.
42. TELUS understands that in the USA, ISPs are currently exempt from the CALEA legislation unless the ISP provides a voice (over IP) service. If this service is provided, then that ISP must provide for CALEA type interception of voice/data.

---

<sup>1</sup> Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications.

TELUS is concerned that Justice Canada is proposing to impose lawful access requirements on Canadian ISPs before U.S. regulatory authorities impose such provisions on American ISPs. This appears to be inconsistent with the Justice Canada statement that it is "essential to ensure that no competitive disadvantages are placed on Canadian industry." This is also inconsistent with the TELUS recommendation above that Canada and its major trading partners should "harmonize" their lawful access provisions rather than set up exclusive "made in Canada" requirements. Harmonization in this regard is still very important, even if Canadian and U.S. ISPs do not compete directly with each other, because manufacturers may not build to meet a unique requirement for a single domestic market. Even if they do, the resulting equipment may be prohibitively expensive and place Canada at a competitive disadvantage in the provision of telecommunications and Internet infrastructure.

43. *TELUS recommends that any new lawful access requirements for Canadian service providers should be consistent with those required for the U.S. market.*
44. In attempting to maintain competitive neutrality, TELUS notes that some service providers like TELUS are under CRTC price-cap regulation and cannot automatically raise prices to pay for their lawful access implementation or operational costs. As well, even if a service provider has the ability to raise prices, it may be effectively prevented from doing so by competitive pressures. Since some service providers operate under a regulatory regime and cannot raise rates, while others do not, the only way to maintain competitive neutrality is for government or the law enforcement agencies to pay for the total costs (capital and operational) of their lawful access needs.
45. *TELUS recommends that if incumbent carriers are compelled to incur costs to meet new lawful access obligations, government should defray those costs, whether capital or operational. Indeed, whether or not service providers are able*

*to raise prices, it should be recognized that the costs for implementing the lawful access regime should not be borne by shareholders or customers of service providers.*

#### **Lawful Access Services Should Be Paid By The Federal Government Or By LEAs**

46. TELUS also notes the principle in the Consultation Document that "the solutions adopted do not place an unreasonable burden on the public." There will be a continuing operational cost to assisting law enforcement in their lawful access activities. These costs to service providers should be borne either directly by the Federal Government from general tax revenues, or by the law enforcement agencies, with recourse to their respective governmental sources of funding. In either case, the general public should ultimately bear the cost through general taxation.
47. As noted previously, it would be unacceptable for the federal government to abdicate its duty to fund its lawful access agenda to ensure the safety of Canadians or to attempt to pass the costs associated with its implementation on to a subset of Canadians, the shareholders or customers of service providers. Implementing the lawful access agenda is a general societal cost required to support the policing and national security needs of all Canadians. Such costs should better be paid out of general tax revenues, as are the costs for police and national security. This would include the payment of all existing and new capital upgrades that service providers are mandated by the government to implement.
48. *TELUS recommends that LEAs pay for the specific lawful access services that they use. However, to the extent that the LEAs require additional funds, this too should be supported by the government, and ultimately by the general taxpayer out of general tax revenues.*

49. Adopting a "user-pay" model for specific lawful access services (e.g., a wiretap) makes the most sense in TELUS' view, because:

- a) LEAs that use lawful access services most frequently will pay the most;
- b) if the services are priced reflecting their costs, their use and value as a law enforcement tool can be properly measured by law enforcement against other policing measures;
- c) each service provider is assured of recovering its costs, without having to adjust its prices from time to time and, in the case of the Incumbent Local Exchange Carriers (ILECs), without having to apply to the CRTC for periodic price adjustments; and
- d) the ILECs, which are likely to be the principal (if not the main) providers of these services, will not have to raise the prices for their telecommunications services, thereby potentially weakening their competitive position vis-à-vis other service providers;
- e) LEAs have to pay for the other products and services that they need to fight crime: e.g. cars, gas, guns, dry-cleaning, and telephone service. In TELUS' view, they should also pay for the services proposed in the Consultation Document.

50. It should be noted that CSIS, the RCMP and a number of other provincial and municipal police forces have acknowledged the operational costs associated with telecommunications carriers responding to their assistance orders and have willingly paid for this service. The prices paid have been negotiated between the parties and an accommodation reached. The negotiated prices have been based on the principle of cost-recovery.

51. Currently, a few law enforcement agencies refuse to pay service providers for court-ordered services, relying on the fact that the order does not require that compensation be paid. It should be noted, however, that these orders are typically obtained on an ex parte basis and the court is not asked to consider whether compensation should be required. If the court were asked to turn its mind to this issue and to consider the cost to the service provider of complying with the order, it is likely that some compensation would be ordered.

52. *TELUS recommends that the proposed legislation expressly require that law enforcement authorities compensate service providers for their reasonable costs of providing lawful access services*

**Prices For Services Should Be Determined Between the "Buyer"( the LEA) and the "Seller" ( the Service Provider)**

53. There has been some suggestion that a standardized list of prices could be set out in regulations by Justice Canada and paid by all law enforcement authorities to each service provider for each service provided, regardless of the costs incurred by that provider in carrying out that service. In TELUS' view, this is not a particularly appropriate or practical mode of operations. TELUS fears that there will be regulatory lags in this system. With the advance of technology, the types of services requested might expand beyond those that are on the price list. As well, the prices specified will be difficult to maintain up to date as actual telecommunications costs change each year. In addition, each service provider has a particular set of equipment and mode of operation. Since each has a different cost structure, standardized prices would not adequately reflect the costs that individual service providers incur. Standardized prices might over-recover for some and under-recover for others. Currently, service providers meet and negotiate pricing for services with law enforcement authorities and arrive at prices that are acceptable to both parties. TELUS opposes a standardized "one-size-fits-all" list of prices for lawful access services in favour of a negotiated set of prices for each carrier. In cases where a negotiated set of prices cannot be reached, TELUS recommends that the issue be resolved by arbitration.
54. *TELUS recommends negotiations between LEAs and service providers to develop cost-based pricing acceptable to both parties. If an agreement cannot be reached, TELUS recommends arbitration.*

## **The Ambit Of The Proposed Legislation**

55. The working definition of a service provider in the Consultation Document is as follows:

"Service Provider" means a person who owns or operates a transmission facility that is used by that person or another person to provide telecommunications services to the public in Canada.

and the working definition of a transmission facility is as follows:

"Transmission Facility" means any wire, cable, radio, optical or other electromagnetic system, or any other (similar) technical system, used for the transmission of information between network termination points.

56. TELUS notes that due to the reference in the proposed definition to transmission facility, some resellers and rebillers of telecommunications services who do not own or operate a transmission facility will be left out of the ambit of the legislation, although they may still have subscribers that are targets of interest for law enforcement. Since resellers and rebillers simply maintain a list of customers and their transmission system requirements are supplied by "service providers" as noted above, TELUS suggests that further thought needs to be given to the ambit of the legislation.

57. During government/industry discussions that took place during the consultation period, consideration was given to exempting certain service providers or whole classes of service providers from the provisions of lawful access where it was determined that those service providers would never have lawful intercept "targets of interest." On the other hand, TELUS is concerned that if the authorities lack the capability to carry out lawful access on certain systems, those operations might attract users who are more likely to be targets of interest for lawful access. TELUS emphatically urges the government to avoid selectively targeting only



certain service providers with its lawful access requirements. Such an "a priori" exemption or narrowing of the obligations would not only seem to compromise the purpose of the lawful access agenda but could violate the obligation to ensure that the lawful access agenda is administered in a competitively neutral manner that does not asymmetrically burden only a particular class of service providers.

58. *TELUS urges the government to provide information on which department(s) would be responsible to "exempt" certain service providers because they might not have "targets of interest" and under what criteria such exemptions would be granted.*

59. The Consultation Document also states "It is crucial that service providers know what is required of them." As noted before, it is equally crucial, in TELUS' opinion, that the Government know its service providers, and can track their lawful access capabilities and any required forbearance. As noted earlier in this response, there is no discussion of how service providers will be tracked in this new regime to see what access standards they can meet, what forbearance is required and for how long, and what penalties might be applied to promote compliance.

**The Lawful Access proposals risk being in conflict with the Government's Innovation Strategy.**

60. TELUS urges the federal government to carefully consider the potential harmful effect on innovation of any proposed legislation or regulation on the provision of new and existing services to Canadians. Proposals that increase the regulatory burden or introduce other costs to be borne by communications companies can delay, or even provide cause to cancel, the introduction of new products and services that connect Canadians and help people embrace the knowledge economy.

61. The Consultation Document proposes a requirement to "provide at a minimum a basic intercept capability before providing new services or a significantly upgraded service to the public." Without having further details on the proposed arrangements, this proposal appears inconsistent with the Government's Innovation Strategy, which seeks to promote new and innovative services for all Canadians. The idea that Canada's telecommunications service providers would be penalized by complying with new government lawful access requirements whenever they improved their services is potentially at odds with the desire to provide new and innovative services for Canadians. Similarly, the idea that the Government would reward those telecommunications service providers who do not innovate is equally inconsistent.
62. *TELUS recommends that the desire to provide new services to Canadians while satisfying the needs of law enforcement be reconciled in such a way as to maintain the innovative nature of our economy, as well as the individual's rights to privacy.*

#### **Need To Reduce Risk And Uncertainty By Defining Terms In A Government/Industry Working Group**

63. TELUS is concerned with the current lack of information available for review. The undefined terms relating to "a basic intercept capability", "network termination points" and "new services or a significantly upgraded service to the public" leave many considerations open to interpretation. In reviewing presentation materials provided in consultation meetings, the outline of a "basic intercept capability" was described, but no description was offered for new and significantly upgraded services, nor of how each service would be assessed and by what process they will be determined to be either "old" or "new." Again, TELUS would like to reiterate its position that an opportunity to review draft legislation and regulations would provide a much better understanding of these matters and a superior foundation for constructive comment.

64. TELUS believes that an "old" service such as PCS wireless provided to a new geographic area in Canada should retain its "old service" status. In such cases, the lawful access already provided in the "old" area would also be extended to the "new" area. Before commenting further, however, on this proposal, TELUS needs much more precise understanding of the terms that the government is using. In support of this Justice Canada initiative, TELUS would be prepared to work with others in industry to provide workable definitions for these terms.
65. *TELUS further recommends that Justice Canada convene a group with industry to work on such implementation guidelines to give clarity and remove the potential for surprises to the industry as it proceeds to offer innovative services.*

**TELUS Proposes Regulation By Reference As Being A Faster, More Flexible Mode Of Operations**

66. TELUS understands that the legislation will set out the policy for lawful access and the powers granted to implement it including provisions for forbearance and sanctions associated with non-compliance. Among the powers will be the power to make regulations, which will detail how the specifics of lawful access will operate. TELUS is concerned with the potential regulatory lags that may be associated with such a regime and suggests that the prescription of technical and other lawful access requirements be developed by government including:
- apparatus to be installed
  - capacity requirements
  - maximum number of simultaneous interceptions
  - terms and conditions pertaining to the security of interception
  - specifications on delivery of the product of interceptions.
67. *TELUS recommends that these specifications be placed in a document referenced by regulation and subject to public comment whenever it is revised. It has been*

*our experience that modifications and updates can be developed much more easily and more quickly in this manor than if regulations must be amended.*

#### **Point Of Demarcation / End Of Service Provider Responsibility**

68. TELUS believes that the service provider's responsibility for lawful access must end at a "point of demarcation". TELUS recommends that, for the purposes of lawful access, that point be situated on the service provider's premises as in the current wireline and wireless environments. The service provider may undertake to deliver the information obtained from a lawful access request to other locations for a fee or consideration at the option of the law enforcement authority that requested the lawful access activity, but that delivery should not be part of the mandated lawful access regime, especially given the geographic challenges in Canada.

#### **Status Quo For Service Provider Personnel Qualifications**

69. TELUS recommends that the status quo for its security personnel continue. The current TELUS practice is that only authorized service provider personnel have access to the particulars of the names, addresses, numbers, etc, of lawful access targets. Warrants and their associated assistance orders are shown only to authorized service provider personnel. At the option of the service provider, warrants/assistance orders can either be retained by them on their premises or exchanged for a "comfort letter" from law enforcement confirming the existence of the court documents/orders and the services requested. Due to the safekeeping requirements for retention of the court documents/orders, TELUS suggests that a "comfort letter" approach is preferable in most if not all cases.
70. TELUS notes the interest of the law enforcement authorities in being able to satisfy themselves with respect to the competence, reliability and deployment of service provider employees. Again, this appears to be a restatement of the status

quo and if this is the case, TELUS does not anticipate any future difficulties. If, however, law enforcement wish to change the existing arrangements so that our security staff must not only meet our own employment criteria, but also those of the LEA, there is a strong likelihood of serious labour relations issues arising including those related to jurisdiction that would hinder such action.

### **Forbearance Is A Necessary Tool Leading Towards Lawful Access Requirements**

71. TELUS supports the establishment of a forbearance framework in order to ensure a level of operational flexibility. As noted in the Discussion paper, forbearance could be used to delay but not remove an obligation to comply with the requirements of the statute or regulations, in whole or in part. TELUS notes, however, that the additional bureaucracy that may accompany a forbearance framework may impede the efficient and cost-effective provisioning of services to Canadians, and urges the Government to consider the level of regulation already existing within the telecommunications sector today, specifically the CRTC, Industry Canada and PIPEDA.
72. TELUS has several recommendations with respect to compliance provisions. First, as noted above, Industry Canada has been carrying out an audit/compliance function annually of its PCS licensees assessing their progress in meeting the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications and offering forbearance in consultation with the Office of the Solicitor General as appropriate. This has proved to be an effective mode of operations since 1996.
73. *TELUS recommends that the compliance regime for the new legislation follow this successful model.*

74. TELUS is concerned with the potential competitive biases that would arise if forbearance is offered to one or two competitors in a field while others who might have felt compelled to proceed to deploy additional staff and financial resources might suffer at a competitive disadvantage for their early efforts.
75. *TELUS recommends that any grant of forbearance on one criterion be offered to all service providers if one of the service providers is unable for some reason to implement for reasons of competitive equity.*
76. TELUS questions what would be done with the current conditions of licence that apply to the PCS licence relating to the requirement to comply with the Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications once the legislation associated with this Justice Canada consultation is passed.
77. *TELUS recommends that those conditions of licence under the Radiocommunication Act be withdrawn when the new access legislation is effective. TELUS also recommends that sanctions that might be applied for non-compliance be determined on an ad hoc basis dependent on the circumstances, the reasons for non-compliance, the risks that might be borne during the non-compliant state and the time-duration of non-compliance.*
78. TELUS trusts that virtually all Canadian service providers will understand the need for and respond appropriately to this lawful access regime and will not be non-compliant without "good cause."
79. TELUS fully supports the proposal to suspend any penalty during the time when staffs of the Departments of Industry and the Solicitor General are considering a request for forbearance. If a decision is made to reject the request for forbearance, adequate time must also be provided to allow the service provider to react and to comply before any sanctions are imposed.

## The Requirement for New Law Enforcement Tools

80. TELUS notes the LEA's interest in amending the Criminal Code to allow them to obtain production orders in specific cases while an investigation is underway and when further charges are anticipated. However, the procedural safeguards should, in TELUS' opinion, be at least as strong as those that currently apply to search warrants, since the purpose of the orders is essentially the same and the privacy of Canadians is infringed to the same degree.
81. TELUS believes that it should be up to the Federal Government to decide what new powers the LEAs need and to make the necessary legislative changes, providing that:
- i) the new provisions are consistent with Charter rights and with other applicable laws and regulations that govern our businesses;
  - ii) TELUS has the existing technical capability to comply (consistent with the Convention on Cybercrime); and
  - iii) TELUS is fairly compensated for our services.

Such new powers could provide for:

- production orders
  - assistance orders
  - data-preservation orders
  - interception orders
82. Where execution of an order requires the assistance of service provider personnel, the legislation should provide for, and require, assistance orders that clarify the nature and extent of the assistance to be provided, so that the personnel can readily and clearly understand what is required of them in each instance. The provisions of the Criminal Code dealing with confirming orders should also be clarified so that service providers will know whether or not it is appropriate to

comply with an out-of-province authorization or warrant that has not been confirmed by a court in the province in which the authorization/warrant is to be executed. (There is conflicting case law on this point.)

83. TELUS notes that the following comments are made on the procedural aspects associated with what our understanding of the aforementioned types of orders might entail, and does not address the civil liberties nor the privacy rights of Canadians in our comments. TELUS notes that these types of orders may attract considerable discussion and comment from various interested parties. The Consultation Document indicates that a data-preservation order is "meant as a stopgap measure to ensure that information vital to a particular investigation is not deleted before law enforcement officials can gather together sufficient evidence to obtain a search warrant or production order." From discussions at the associated government/industry consultation meetings, TELUS surmises that a preservation order is an order to "not delete any files or holdings or data on a named individual that TELUS had in its possession prior to receiving the order". Assuming this interpretation to be true, 90 days seems to be an ample term for this "stop-gap measure" until law enforcement can serve a service provider with a search warrant, particularly due to the need for time to deal with international law enforcement coordination. If an extension is required, the Courts should require presentation of argument or further evidence supporting the extension.
84. TELUS also wishes to bring to the attention of Government the difficulties of giving effect to preservation orders on certain types of data such as voice mail. There would be substantial costs and engineering efforts required to retain material such as voice mail when the target in the normal course of his activities routinely deletes it. Since there could be a substantial volume of such information that accumulates over a Justice Canada suggested 90-day "hold" period, it is unclear what system could be used to retain it. TELUS notes that the fulfillment



of preservation orders may not be a trivial matter, as noted above in relation to the various means by which voice mail services may be delivered to Canadians.

85. In TELUS' view, as noted above, virtually all service providers will be trying to do "the right thing" to meet the needs of law enforcement in retaining material noted in a preservation order and for this reason, there seems to be little need for a stated penalty for non-compliance. TELUS notes that there is no stated penalty now in the Criminal Code, and we are unaware of any compliance issues that have arisen. In cases where it might be warranted, a judge could always consider finding a service provider in contempt of court where non-compliance was both deliberate and flagrant.

86. TELUS operates as an ISP and therefore operates servers used by its subscribers for storage of their own data. TELUS' operations in this matter are analogous to those of the operator of a self-storage facility. The provider of storage space rents access and protected storage space, but generally does not know what its customers store and generally bears no responsibility to inspect or search material stored. In its storage contract with the customer, clauses include a prohibition on undertaking illegal operations. Under such circumstances, the self-storage operator assumes no liability if it is later found out that his customer has stored illegal material. Similarly, with reference to the Justice Canada proposals,

87. *TELUS recommends that*

- *an ISP should not attract any liability if one of its subscribers stored a computer virus on its server*
- *there be no onus on ISPs to search out what's stored on their servers to ensure that they are "clean" of viruses;*
- *any legislation or regulations make this explicitly clear*

*Due to the costs of mounting a defense and the diversion of time and talent from other work related activities, TELUS strongly recommends the legislation deal*

*with this issue so that no ISP should ever have to defend itself against any such charges and the potential invasions of privacy that might be associated with such searches.*

#### **Identification Of Local Service Provider And Customer Reverse Directory Service**

88. TELUS has investigated mechanisms that may be useful in providing law enforcement and national security agencies with up-to-date and accurate Customer Name and Address (CNA) and Local Service Provider Identification (LSPID) information while respecting the privacy of its subscribers.
89. TELUS is aware that the Canadian Numbering Administration Consortium Inc. (CNAC) will, in part, respond to the stated needs of law enforcement to link a telephone number to its service provider. By December 2002, as directed by CNAC, the Canadian Numbering Administrator will provide on its website, <http://www.cnac.ca/>, a listing of NPA – NXX's and the code holder (almost always the service provider) for each. For example, 613 728 is a NPA – NXX combination used in Ottawa – Carleton to provide local telephone service and the code holder is Bell Canada. Once instituted, anyone who wishes to consult the website will be able without charge to identify the service provider. This is referred to as the National Numbering Index, or NNI. It is also worth noting that this information is already publicly available on the Telcordia NPA/NXX database.
90. TELUS notes that there is also a Bell Canada tariff which allows law enforcement authorities under CRTC-specified conditions to access an enhanced NNI which also reflects the impacts of local number portability and can therefore provide the service provider for each line number NPA – NXX - XXXX in the country.

## Set-Up Of A Reverse Directory: Telephone Number = Name And Address

91. TELUS, along with other telephone companies in Canada, operates a Directory Assistance service today for wireline-listed subscribers, and Canada wide directories are also freely available via the Internet. TELUS understands that the law enforcement authorities are requesting a "reverse directory" service from which they can get a current name and address if they provide a phone number. TELUS surmises that law enforcement would like to see the establishment of a directory and reverse directory maintained in a more current state than what may be available today for wireline listings posted on the Internet. TELUS considers the following criteria critical in considering the establishment of such a company-specific database:

- TELUS will retain and control its own company-specific database of wireline customers and provide lawful access to it in accordance with the current regulatory regime.
- The incremental costs to maintain and update the information in this database to meet law enforcement service level requirements of timeliness should be borne by the user, the law enforcement community.
- For wireline telephone customers, provision to LEAs of name, address and number information that is already available in a telephone directory or via Directory Assistance should not require a warrant. However, provision of non-published customer information should still require a warrant.
- A degree of coordination will be required between the Justice Canada legislative and regulatory provisions and existing CRTC decisions in this area to decide what customer confidentiality conditions and standards should apply. These should be consistent for all service providers.

92. With respect to the set-up of a company-specific database for wireline listings, TELUS would not ensure any level of accuracy of customer name and address beyond what is currently required by its commercial operations with its customers. TELUS opposes any external obligation to impose an augmented accuracy requirement.

## **Opposition To Collection Of Personal Subscriber Data Unnecessary For Service Provision**

93. TELUS strongly objects to any obligation to collect CNA information if we have no corporate purpose or use for the information collected. While the Consultation Document asks whether a service provider should be compelled by law to collect CNA information, Parliament has already answered this question when it passed the PIPEDA legislation. In that legislation, there is an admonition against collecting unnecessary personal data and a further admonition against retaining such data on file beyond when it is needed.
94. Some telecommunications services that have been and are currently in use in Canada are offered on a "prepaid" or "cash" basis and, as with any other cash transaction, there is a degree of anonymity and no requirement for the establishment of credit or the need to verify identity. Prepaid calling cards may be used to place calls from any phone. They are available today in thousands of retail outlets across Canada. Similarly, a prepaid wireless phone may be purchased, activated and airtime bought without any external verification of the identity of the user.
95. There are well over 4 million wireless prepaid users in Canada today. Limiting the number of outlets where a prepaid calling card may be purchased or where a wireless prepaid cell phone may be activated to those where a service provider can check photo-ID of the intended user would entail a significant change in service operation. It would be ineffective, in any case, since there would still be no way for a service provider to verify the actual users of after-market resold wireless handsets or cards. TELUS notes that there is a market for used wireless phones, which can be purchased and reused along with prepaid service without the knowledge or approval of the service provider.

96. It is important to realize that the imposition of a mandatory information collection rule would radically change the way in which Canadians currently use both prepaid wireless services as well as prepaid calling cards. Implementation of lawful access requirements should not change the way telecommunications services are offered to or used by Canadians.
97. *TELUS recommends strongly against any obligation to collect, maintain or guarantee the accuracy of CNA information if the company has no corporate purpose or use for the information.*

#### **Which Address Is Important In Customer Name And Address?**

98. TELUS also notes the lack of clarity in the proposal to establish a CNA database, in that the type of address is not specified. There is an apparent assumption that there will be a listing of service address, while no consideration is given to the large number of client accounts which have only billing addresses. While service addresses exist for wireline services, it must be emphasized that service addresses for Canada's over 13 million wireless users do not exist. Only a billing address exists, and due to the large number of clients which are businesses, the billing addresses may be in different cities or provinces than the location of the handset. If the name, address and service database referred to in the Consultation Document is to be used to geographically locate certain individuals by law enforcement authorities, it is not likely to be useful for the growing number of clients that have opted to forego their traditional wireline subscription for wireless or certain other technologies.

#### **A Distributed Service Provider CNA Database With National Coordination Makes Most Sense**

99. The establishment of a single national subscriber database is an extremely costly and complex undertaking since it must be maintained and updated by local service

providers to retain its validity. Service providers cannot vouch for the accuracy of a national database without a major revamp of the ways in which telecommunications services can be provided in Canada. There is no way of continually verifying its accuracy. In TELUS' view, this national database, if implemented, would have the largest number of records and the largest update requirement of any database ever attempted in Canada. A series of service provider databases, to which access is controlled and coordinated through an independent national body, seems to be a much more practical alternative if law enforcement insists that such a database service is needed.

100. *TELUS recommends that if the establishment of databases is determined to be a requirement, service provider databases be set up separately by each service provider containing the name and address data associated with wireline telephone service only.*

**CNA National Coordination Is Best Left To Operation By A Third Party Industry Consortium**

101. Since the proposed national coordinator would have direct access to the confidential customer lists and contact information for all Canadian service providers, it could not be operated directly by a service provider. Similarly, law enforcement authorities should not operate it, since it will contain some confidential (non-published, non-listed wireline name and address) data, and this confidential data should only be available to law enforcement with judicial authorization.
102. *If it is determined that a CNA database is required, TELUS recommends that its operation for law enforcement purposes be coordinated by an independent third party, separate from law enforcement and separate from service providers.*

103. The CRTC and the telecommunications industry have had extensive experience in setting up such independent corporate entities following the introduction of local competition in the telecommunications market. Three third-party corporations were set up by industry in 1998, namely:

- the Canadian Numbering Administration Consortium Inc. (CNAC) responsible for the administration and assignment of the numbering resources in Canada;
- the Canadian Portable Contribution Consortium Inc. (CPCC) responsible for collecting funds for all telecommunications service providers as per the rates specified by the CRTC and for distribution of those funds to local exchange carriers as per CRTC rules on disposition; and
- the Local Number Portability Consortium Inc. (LNPC) responsible for the operation of the LNP database and access to it.

104. These are three ready examples of companies set up at arms-length from the industry to provide common services to each telecommunications service provider. Models of their corporate governance are available from the CRTC or from their executives.

105. *TELUS recommends study of these companies as possible models for the set-up and operation of a network for law enforcement to access customer name and address information under specified controls administered by the third party operator.*

106. In summary, TELUS has a long history of cooperating with the law enforcement agencies and in aiding them to carry out their lawful mandate. TELUS recognizes that lawful access is an essential tool for national security and law enforcement and understands the challenges to LEAs that have prompted the issuance of this Consultation Document. TELUS hopes that its comments and recommendations will help the Government to develop appropriate responses to those challenges.

## Conclusions and Recommendations

107. *TELUS recognizes that lawful access is an essential tool for national security and law enforcement.*
108. *TELUS urges the government to harmonize its requirements with those in other countries, particularly with those in the U.S. to help reduce the costs of provisioning and to ensure that Canadian industry is not disadvantaged competitively by unique "made in Canada" requirements.*
109. *TELUS recommends that sufficient federal funding be made available to service providers:*
  - *to retrofit all networks and systems to satisfy all lawful access needs of LEAs;*
  - *to cover all incremental costs to provide the capability for lawful access to new networks and systems providing upgraded, significantly enhanced and new services; and*
  - *to pay service providers, as necessary, for their operational costs to provide all lawful access services that may be requested by local, regional and national law enforcement authorities.*
110. *TELUS recommends that Justice Canada release a draft bill and its associated regulations for public comment and input prior to proceeding to Parliament for first reading of a Bill.*
111. *TELUS recommends that lawful access capabilities be required in all new equipment being considered for introduction to the Canadian telecommunications market place, which will be used for the provision of voice or data services.*
112. *TELUS recommends that if incumbent carriers are compelled to incur costs to meet new lawful access obligations, government should defray those costs, whether capital or operational. Indeed, whether or not service providers are able*



*to raise prices, it should be recognized that the costs for implementing the lawful access regime should not be borne by shareholders or customers of service providers.*

- 113. TELUS recommends that LEAs pay for the specific lawful access services that they use. However, to the extent that the LEAs require additional funds, this too should be supported by the government, and ultimately by the general taxpayer out of general tax revenues.*
- 114. TELUS recommends that the proposed legislation expressly require that law enforcement authorities compensate service providers for their reasonable costs of providing lawful access services*
- 115. TELUS recommends negotiations between LEAs and service providers to develop cost-based pricing acceptable to both parties. If an agreement cannot be reached, TELUS recommends arbitration.*
- 116. TELUS urges the government to provide information on which department(s) would be responsible to "exempt" certain service providers because they might not have "targets of interest" and under what criteria such exemptions would be granted.*
- 117. TELUS recommends that the desire to provide new services to Canadians while satisfying the needs of law enforcement be reconciled in such a way as to maintain the innovative nature of our economy, as well as the individual's rights to privacy.*
- 118. TELUS further recommends that Justice Canada convene a group with industry to work on such implementation guidelines to give clarity and remove the potential for surprises to the industry as it proceeds to offer innovative services.*

119. *TELUS recommends that these specifications be placed in a document referenced by regulation and subject to public comment whenever it is revised. It has been our experience that modifications and updates can be developed much more easily and more quickly in this manner than if regulations must be amended.*
120. *TELUS recommends that the compliance regime for the new legislation follow the successful model, which has been used in tracking the lawful access compliance of Personal Communications Service licensees since 1996.*
121. *For reasons of competitive equity, TELUS recommends that any grant of forbearance on one criterion be offered to all service providers if one of the service providers is unable for some reason to implement.*
122. *TELUS recommends that the lawful access conditions of licence under the Radiocommunication Act applicable to Personal Communications Service licensees be withdrawn when the new lawful access legislation is effective.*
123. *TELUS recommends that sanctions that might be applied for non-compliance be determined on an ad hoc basis dependent on the circumstances, the reasons for non-compliance, the risks that might be borne during the non-compliant state and the time-duration of non-compliance.*
124. *TELUS recommends that:*
- *an ISP should not attract any liability if one of its subscribers stored a computer virus on its server*
  - *there be no onus on ISPs to search out what's stored on their servers to ensure that they are "clean" of viruses;*
  - *any legislation or regulations make this explicitly clear.*

125. *TELUS recommends strongly against any obligation to collect, maintain or guarantee the accuracy of CNA information if the company has no corporate purpose or use for the information*
126. *TELUS recommends that if the establishment of databases is determined to be a requirement, service provider databases be set up separately by each service provider containing the name and address data associated with wireline telephone service only.*
127. *If it is determined that a CNA database is required, TELUS recommends that its operation for law enforcement purposes be coordinated by an independent third party, separate from law enforcement and separate from service providers.*
128. *TELUS recommends study of the three consortium companies (CNAC, CPCC and LNP) as possible models for the set-up and operation of a network for law enforcement to access customer name and address information under specified controls administered by the independent third party operator.*

Pierlot, Paul

---

From: [REDACTED]  
Sent: 2002 Dec 16 6:11 PM  
To: la-al@justice.gc.ca  
Subject: Lawful Access consultation response

s.19(1)



Lawful access

final.wpd

Please find attached the response of the BC Civil Liberties Association to the consultation document on Lawful Access. If there are any problems opening the attachment, please contact me directly.

Thank you  
vg

[REDACTED]  
B.C. Civil Liberties Association  
425 - 815 West Hastings Street - Vancouver, B.C. - Canada - V6C 1B4  
(604) 687-2919 | [REDACTED] | [www.bccla.org](http://www.bccla.org)

**Comments by the B.C. Civil Liberties Association  
to the  
Department of Justice  
December 16, 2002**

**RE: Lawful Access - Consultation Document**

**Introduction**

The B.C. Civil Liberties Association (BCCLA) is the oldest and most active civil liberties group in Canada. We are a group of citizens who volunteer our energy and talents to fulfill our mandate: to preserve, defend, maintain and extend civil liberties and human rights in British Columbia and across Canada. We are a charitable, non-profit society.

Privacy is an important part of the BCCLA's mandate. Over the years, we have become a leading advocate for the privacy rights of British Columbians and we have been involved in number of high profile dossiers in this area, including the Anti-terrorism Act and the API-PNR database.

Before providing our substantive comments, we wish to note that the consultation document is quite vague about what the government of Canada is actually proposing. Other than a few suggested definitions, the consultation document is couched in generalities and lacks specifics about what measures the government plans on instituting. Because of this, our comments will necessarily be at a similar level of abstraction. We look forward to the opportunity to respond to whatever legislative proposals are brought before a parliamentary committee.

**Why does the government believe the proposed action is necessary?**

The Consultation Document sets out three general rationales for the proposals being made.

***Rapidly evolving technological environment***

The first is the rapidly evolving telecommunications environment, which the paper says "can make it more difficult to gather the information required to carry out effective investigations." p.

The principal difficulties appear to be technological, and the paper cites new calling options for wireline communications, expansion of wireless communications and the Internet as areas where law enforcement and national security organizations have had difficulty in gaining access to data. The government proposes placing requirements on service providers to facilitate this access.

In fact, at the Vancouver consultation meeting with government officials, an often repeated theme was that the government was looking to "shift the costs" of surveillance onto service providers directly and onto citizens indirectly if service providers opt to pass along these costs to consumers.

Page -2-

This would be a remarkable shift in approach from current practice, where surveillance of citizens is carried out by law enforcement or security agencies and their costs are considered to be the costs of doing the job Parliament has assigned them. Parliament allocates funds for these activities and the agencies are expected to live within their budgets. What is being proposed is a form of licensing fee on service providers who will be required to assume these costs in order to be allowed to operate.

This is not so much a simple response to technological developments that would allow continuation of current practices as a seismic shift in how surveillance is carried out and paid for. The fact that new technologies pose challenges for law enforcement and security organizations does not justify what is being proposed. The government must show clearly that there is no way that the current system can operate, not that it will cost more money or be inconvenient for those doing the monitoring of citizens.

#### *Implementation of the Council of Europe Convention on Cyber-crime*

The second rationale being put forward by the government is the need to ratify the Council of Europe Convention on Cyber-crime. This treaty is the latest in a series on mutual legal assistance, and is designed to facilitate combating international computer and Internet-based crime, including child pornography, propagation of viruses, on-line fraud, etc.

The Consultation Document states that most of the legislative authority already exists in Canada, but that three additional measures would have to be added to the Criminal Code before Canada can ratify the treaty. These are:

- provisions for a production order;
- provisions for a preservation order; and
- an offence in relation to computer viruses not yet deployed

These are not minor amendments. The notion of a preservation order is unknown in Canadian law, and would be a major shift in Canadian criminal law and a bigger incursion into the privacy of Canadians. This goes well beyond simply maintaining existing lawful access capabilities.

Production orders are a very limited concept in the Criminal Code, and the proposals appear to propose a huge expansion of their use and availability. Again, we are looking at major changes to Canadian criminal law and bigger incursions into the private lives of Canadians.

The government says these power are needed to fight crimes against the Internet or crimes being carried out using the Internet, and we have to do this in order to ratify the treaty.

Page -3-

It should be noted that the Convention on Cyber-crime has been in existence for barely a year, with 34 states (including Canada) having signed it. For the Convention to enter into force five countries must ratify it, including three member countries of the council of Europe. To date, only Croatia and Albania have ratified the treaty.

This means the Convention is not yet in force, and the government has not indicated when this is likely to happen. If there is no functioning treaty to take part in, Canadians should take the time to carefully consider the implications of what is being proposed for their historic civil liberties.

Furthermore, the treaty provides for reservations by federal states. None have been filed as yet, but the United states has not ratified the Convention. We do not know which states may seek reservations from some provisions of the treaty. It would be prudent for Canada to see what its largest trading partner and the country with which we are most closely integrated in terms of our communications system is going to do and respond appropriately.

Finally, we raise the difficulty we have with the argument that otherwise unjustifiable policy changes must be made because a treaty requires that we do it. There is a high risk of policy laundering, where a government seeks to avoid or sidestep scrutiny (and the consequent criticism and political cost) by legislatures, the media or the public by saying "the treaty made us do it."

#### *Public policy objectives*

The consultation paper refers to the 2001 Speech from the Throne (SFT) as promising action to deal with cyber-crime, a promise the government argues it is keeping by bringing in these proposals. The relevant section of the 2001 SFT is reproduced below.

"The Government will focus on safeguarding Canadians from new and emerging forms of crime. It will provide enhanced law enforcement tools to deal with emerging threats to security, such as cyber-crime and terrorism. It will act to safeguard children from crime, including criminals on the Internet."

However the Consultation Document does not refer to another part of the SFT, which actually precedes the pledge on cyber-crime. It is reproduced below.

"It will also modernize federal privacy law to safeguard the personal information of Canadians and provide better copyright protection for new ideas and knowledge."

The 2001 Throne Speech actually acknowledges the need for a balance between the need to fight crime on the Internet and protect the privacy rights of Canadians. To date, we have not seen any action on this pledge. This speaks volumes about the priorities of the government, especially when considered in light of the various measures which have been taken to restrict and infringe the privacy rights of Canadians in the name of the fight against terrorism.

#### **The Right to Privacy Generally**

Page -4-

The BCCLA position on the right to privacy, with respect to surveillance by state agencies, runs on two parallel lines.

These two tracks were set out by the Supreme Court of Canada in *R. v. Dymont*, in the following words:

"Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state." *R. v. Dymont*, [1988] 2 S.C.R. 417, at pp. 427-8.

Human beings prize privacy as one of the essential features of a liveable environment. Being subject to relentless scrutiny, particularly when that scrutiny involves the vast resources and punitive powers of a state, makes for less human happiness. The ability to communicate to our fellow human beings freely and without the fear of any or every word we utter being recorded and scrutinized is essential for human dignity and even human health, both physical and mental. A system which would permit government and its agents to monitor all our electronic conversations would greatly diminish human happiness and human health.

It would also diminish and reduce our democratic society.

The BCCLA has a fundamental commitment to "forum democracy" as centred on a self-governing, deliberative citizenry. The People are the ultimate source of political authority in a democratic polity. Meiklejohn's resonant battle-cry: "they must be free because they must govern" refers to the symmetry between the limited free speech privileges of legislative bodies and the limited free speech privileges of the citizenry in their forum. The BCCLA contends that this symmetry also extends to the limited privacy privileges of the executive tribunals of a democracy and the limited privacy privileges of the citizenry in their forum.

Executive privilege turns on the conviction that, without privacy protection, executive bodies are unable to discharge their duties. With every musing and speculative line of thought open to scrutiny and misinterpretation, it would be practically impossible for an executive to operate. The courts in Canada and elsewhere have repeatedly affirmed this principle, most recently in *Babcock v. Canada (Attorney General)* 2002 SCC 57. File No.: 28091, and have declined to allow citizens or the media access to documents which could reveal these inner private discussions among cabinet ministers.

Similarly, the ultimate rulers of the country are the people, and they must be free to discuss all matters freely, and without fear of monitoring, if the forum of the ruling citizenry is to have the uninhibited vigour it needs.

The right to privacy in law



Page -5-

The proposals contained in the Lawful Access consultation document engage the protections of privacy contained in the Charter of Rights and Freedoms.

The Supreme Court of Canada has repeatedly affirmed, in a number of different contexts (search warrants, (*R. v. Plant*), income tax audits/investigations (*R. v. Jarvis*, *R. v. Ling*) possession of child pornography (*R. v. Sharpe*) or blood samples (*R. v. Dymont*) that the Charter will protect the right to privacy. It has affirmed the privacy rights of Canadians under both s.7 and s.8 of the Charter, as well as under statutes and the common law.

*Section 7:*

Section 7 reads as follows:

7. Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

A central principle of fundamental justice is that the individual's interest of privacy cannot be unreasonably interfered with by the state. In *R. v. Sharpe*, 2001 1 S.C.R. 45, the Court recognized that "freedom from state intrusion and conformist social pressures is integral to individual flourishing and diversity", and also stated that "Privacy, while not expressly protected by the *Charter*, is an important value underlying the s. 8 guarantees against unreasonable search and seizure and the s. 7 liberty guarantee." (At para 26)

In the context of the lawful access proposals, these values as state are clearly of the highest order. They are individual communications for which individuals assume the state will not be monitoring. Likewise, traffic data being considered for protection and production orders is so intimately connected to the privacy of the individual that the highest level of protection must be in place to protect it. The "full panoply" of Charter rights will undoubtedly be engaged to protect the individual from such surveillance.

*Section 8:*

Section 8 of the *Charter* provides that:

8. Everyone has the right to be secure against unreasonable search or seizure.

In fact, section 8 protects a reasonable expectation of privacy. What makes up a reasonable expectation of privacy will depend on the context, and "an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement" (*Hunter v. Southam Inc.*, *supra*, at 159-60, *per* Dickson J. (as he then was).

"The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether it is

Page -6-

expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates that an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement." *R. v. Dyment*, [1988] 2 S.C.R. 417, at 428.

The Supreme Court has looked at the reasonable expectation of privacy in a number of different contexts. They have held that commercial documents may include a reasonable expectation of privacy (*Thomson Newspapers*), but this may be lower than for personal information, especially when those documents are produced for regulated activities. It was also held that there was a reduced expectation for Employment Insurance information (*R. v. Smith*) and documents prepared for tax purposes, since they are subject to audit. "taxpayers have very little privacy interest in the materials and records that they are obliged to keep under the ITA, and that they are obliged to produce during an audit." (*R. v. Jarvis*)

The Consultation Document cites the decision of the Supreme Court of Canada in *R. v. Plant*, [1993] 3 S.C.R. 281 to support its view that subscriber traffic data is subject to a lower level of protection under s.8 than content or conversations or e-mails. In fact, the case says something very different.

In *R. v. Plant* at 293, Sopinka J. listed several factors that will determine the parameters of the protection afforded by s. 8 with respect to informational privacy. These include consideration of such factors as :

- the nature of the information itself,
- the nature of the relationship between the party releasing the information and the party claiming its confidentiality,
- the place where the information was obtained, the manner in which it was obtained, and
- the seriousness of the crime being investigated

*Plant* involved a marijuana grow-operation in a residential house. The police received a tip about the operation, did a perimeter search of the house, which they noticed had covered windows (a common characteristic of grow-ops). They used a computer to gain access to the hydro records of the house, which were four times higher than normal for a similar sized house in the city. This access to customer records was granted to police by Calgary Hydro on an on-going basis. The police obtained a search warrant and charges followed.

The constitutionality of the various searches were challenged by the accused, but for the purposes of this discussion the computerized hydro records are the most relevant.

Sopinka, J stated that section 8 seeks to protect "a biographical core of information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state." (at 293). He also wrote that this is the type of information "which tends to reveal intimate details of the lifestyle and personal choices of the individual."

Page -7-

In *Plant*, the court held that hydro records were not the kinds of information which a client would have a reasonable expectation of privacy. Significantly, Sopinka J. drew the distinction between the hydro records and records maintained in the personal computer of a private citizen, but also noted that the records in *Plant* were "close to the line". McLachlin J., (as she then was) concurred in the result, but was of the view that the search of the hydro records crossed the line and a warrant was required to gain access to them. This was because "the very reason the police wanted the records was to learn about the appellant's personal lifestyle." (at 302)

It is submitted that the records to which the lawful access proposals would apply are closer to those on an individual's computer than they are to hydro records, as McLachlin J. indicated in *Plant*:

"Computers may and should be private places, where the information they contain is subject to legal protection arising from a reasonable expectation of privacy. Computers may contain a wealth of personal information. Depending on its character, that information may be as private as any found in a dwelling house or hotel room." (at 303-04)

In fact, the records proposed and electronic conversations which the government has identified under its Lawful Access proposals are closer to telephone conversations than they are to files on a computer hard drive. The way Canadians use e-mail is much closer to the way they converse on a telephone than an exchange of letters. Cellular phone records can show a person's movements from one cell zone to another. Records of surfing of the Internet would reveal some of the most intimate details of a person's private life.

For all these reasons, we are of the view that the electronic interception proposed in the Consultation Document should be given the highest level of protection, equal to the interception of private communications (wiretaps). Anything less would be a diminution of Canadians' privacy rights.

#### **What is being proposed? What is the extent of the infringement being proposed?**

The overall scheme being proposed is a radical reordering of how surveillance is carried out in this country. All service providers will be required to ensure that the authorities of the state will be able to monitor various types of electronic communications.

The first step to be taken by the authorities would be a preservation order which would require the service provider to "store and save existing data that is specific to a transaction or client." at 13 This is supposed to be a temporary measure until authorities would be able to get a proper judicial order. It would be approved either judicially, or in "exigent circumstances" by the law enforcement agencies directly without a judicial order.

A production order would be judicially authorized and it would require the service provider to

Page -8-

deliver the data to law enforcement officials within a certain period of time. The Consultation Document foresees two types of production orders.

A general production order would be the equivalent to a search warrant, and require the production of documents.

A specific production order would apply to traffic data, and the Consultation document states that this and other traffic data is subject to a lower expectation of privacy.

The BCCLA has a number of points of contention with this approach.

First, we do not accept that a search of electronic communications information as part of a criminal investigation involves a lower expectation of privacy at any point. As indicated in *R. v. Plant*, computer information is much more personal than hydro records, which the court found were a borderline case and close to the edge for requiring a warrant to be examined. Certainly, there should never be an order issued for the preservation or either traffic or content data on the simply say-so of law enforcement authorities.

We also share the concern expressed by the Privacy Commissioner of Canada that the two-part process between judicial authorization of a preservation order and a production order could result in a situation where neither judge conducts the rigorous examination of the allegations supporting the application for the order, on the assumption the other judge has/will do it.

It is apparent that preservation orders pose a great threat to civil liberties, and the Consultation Document's proposals do not provide anywhere near sufficient safeguards for this radical concept to be incorporated into Canadian criminal law.

The proposal for production orders also betrays a view that the collection of communications data is only slightly more intrusive than monitoring hydro consumption records. However, as the Supreme Court stated in *Plant*, hydro records themselves are a borderline case, so it appears anything beyond that would entail a reasonable expectation of privacy and the full range of protections under the Charter.

As for retention orders, we will not outline our views as officials have indicated that retention orders are not being planned by the government. However, we wish to state that the concerns we have expressed regarding preservation orders would be increased exponentially if retention orders are being contemplated either now or in the future. We also express some pessimism on this point given the actions of some other signatories to the Convention on Cyber-Crime, specifically the United Kingdom, to set up a system of data retention.

#### **What legal and practical safeguards will be in place?**

Article 15 of the Convention provides for the parties to adhere to certain minimum safeguards for the protection of human rights.

##### **Article 15 – Conditions and safeguards**

1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards

Page -9-

provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest, in particular the sound administration of justice, a Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

The Consultation Document does not talk about safeguards except in generalities such as "the need for effective measures that balance the rights, privacy, safety, security and economic well being of all Canadians." (p.5) As noted above, the proposals exhibit a cavalier attitude to the privacy rights of Canadians, particularly with regard to communications traffic data.

It is strongly recommended that the traditional and proven safeguard of judicially authorized warrants be used where the government can justify the need for such warrants.

**How likely are the new measures to achieve the desired result?**

It seems unlikely that the measures being proposed will have the effect of reducing significantly the types of organized criminal activity set out in the consultation document. There are two principal reasons for this belief.

### *Strong encryption*

If these proposals are enacted, it will become much more common for anyone using the Internet to use various types of encryption if they are interested in maintaining a degree of personal privacy. This is going to become increasingly common as people become more and more aware that their e mails are subject to intercept for a variety of reasons.

For criminals and terrorists, it can be safely assumed that if they are at all organized, they will

Page -10-

already be using encryption for electronic communications related to their criminal activity. This will mean that the government will primarily be able to intercept the communications of low-level criminals, or individuals who are downloading pornography or discussing minor criminal activity.

To go after the big fish, the government will have to come back with new proposals prohibiting the use of encryption by everyone. That is the next logical step following the new philosophy that the citizen must ensure the state is able to eavesdrop on any and all conversations.

*Criminals likely to move to private networks to avoid detection*

Organized crime and terrorists are also likely to avoid the whole realm of service providers and public networks by setting up their own private networks to send electronic communications among themselves. This will have the effect of avoiding all the measures now being proposed by the government. If the use of private networks becomes widespread, the government will have to bring in new legislation to address the communications of criminals and terrorists.

**Other recent incursions by government on the right to privacy**

These proposals for lawful access are only the most recent government action which dramatically reduces the privacy rights of Canadians. The following section sets out the context in which these proposals are being made, and it shows a relentless incursion into the privacy rights of Canadians.

*The Anti-terrorism Act*

The *Anti-terrorism Act* contains extraordinary forms of lawful interception of telecommunications. While the Consultation Document considers the routine requirement of judicial authorization for the lawful access of enforcement authorities to private communications, it ignores the extraordinary powers now legally vested in CSIS and the Communications Security Establishment to undertake surveillance at the sole behest of the Minister of National Defence. Further, Bill C-36 explicitly provided for the OPERATIONAL integration of CSE assets and police authorities.

Now that the enormous electronic sigint assets of the CSE have been turned toward domestic targets, it faces new challenges of scale, and the proposals are very much concerned to facilitate an enormous scaling-up of the Government's surveillance activities. Consider, for instance, the suggestion that preservation orders be in force for a minimum of 90 days while the government seeks judicial authorization to intercept specific communications. Such a huge period of time makes no sense in "specific" cases, but eminent sense in those circumstances where the government is seeking wholesale access to entire groups of communications which will be machine-screened for suspicious contents.

Page -11-

We must note that in the Moussaoui and similar cases, the identification of a terrorism suspect often only occurs *after* they act. A 90 day preservation order at that time will often yield nothing, logically leading the government to expand its preservation requirements into retention requirements.

#### *The Public Safety Act (Bill C-17)*

This legislation, which is now before a legislative committee, would also have the effect of opening the private lives of Canadians to greater government scrutiny. RCMP officers would have access to the AIP-PNR database for the purpose of transportation security which identifies a number of different personal characteristics of air passengers.

This database already provides access to air passenger data for the Canada Customs and Revenue Agency (CCRA) which is able to retain it for 6 years and use it for a variety of purposes. It has also been expanded to include information on passengers using other means of transportation. We have already voiced our concern about this database to the minister responsible, as have a number of other groups and the federal and several provincial Privacy Commissioners.

#### *Other measures*

The creation of the Total Information Awareness Program in the United States is also a great concern, given the amount of data from Canada which either flows through or is processed in the United States. This system is designed to collect and retain the maximum amount of personal information available on everyone, then sort it for various patterns of behaviour.

Such a system is abhorrent, and it goes well beyond what is being proposed in this document. However, given the various linkages between security and law enforcement agencies in our two countries, we wonder how long it will take for Canadian agencies to have their American colleagues do their electronic surveillance for them.

## CONCLUSION

In the final analysis, we are not convinced that these proposals should go forward.

There has been no need demonstrated which would justify the massive intrusion into the private lives of Canadians and the reversal of protections against unreasonable search and seizure. The government simply states that it is more complicated to conduct electronic surveillance, not that it is impossible to do. The Council of Europe Convention on Cyber-crime is not in effect, and there is no indication

Page -12-

that it will be anytime soon. We also don't know what reservations might be made under the treaty by other federal states, including some of our closest allies and trading partners. A vague promise made in the Speech From the Throne before last is also a less than convincing rationale for allowing huge incursions into our civil liberties.

In addition to being a massive intrusion, these proposals would also require Canadians and/or their service providers to pay for the surveillance being conducted on them and their fellow citizens. This philosophy reached its absurd final result in Germany this year when customers subject to wiretaps were billed for this 'service'. What the Government of Canada is proposing here is that everyone will be billed, but only some of us will be bugged.

This is wrong in principle and will be impractical in operation.

The lack of safeguards for privacy are also disturbing, as is the expressed view that traffic data is somehow not revealing of a person's private life and therefore not worthy of protection.

We are also unconvinced that what is being proposed here would actually help fight organized crime or terrorism. What is more likely is that agencies of the state will have much more access to the private lives of ordinary Canadians, and will prosecute some of them for looking at forbidden material or having unguarded electronic conversations. Serious criminals and terrorists are unlikely to be careless enough to fall within the ambit of these proposed measures.

This brings us to the other shoe, which will drop once it becomes apparent that these 'lawful access' measures are insufficient for the government's purposes. We will then see legislation banning encryption, restrictions on private networks as well as data retention orders. These will all be justified on the same flimsy basis as these proposals.

Whatever speculative (and we stress the word speculative) advantage might be gained for law enforcement and security authorities by the legislative measures proposed in this consultation document, the acceptance of its proposals would have the certain effect of sweeping away the privacy rights of Canadians in the electronic sphere without having a significant effect on crime or terrorism.

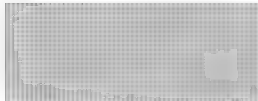
Requiring the citizenry - at their own cost - to only communicate in ways that facilitate state surveillance, and to provide for at least partial records of all of their digital communications, strikes at the heart of both civil and human privacy rights. It envisages a body of law that prohibits communication at a volume lower than a stage whisper, lest government agents meet with difficulty in eavesdropping; and also requires the citizenry to record their conversations against the contingency that the state may wish to refer to them at some later time. This is *fundamentally* wrong, and we will use every resource available to us to fight it root and branch.




Page -13-

For more information, contact:

s.19(1)



B.C. Civil Liberties Association  
425 -815 W. Hastings St.  
Vancouver, B.C.  
V6B 1C4  
(604)687-3013 tel.  
(604) 687-3045 fax  
email: 

K:\CLW\Board\POLICY\EB8\Lawful access final.wpd

Pierlot, Paul

---

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 16 6:47 PM  
To: la-al@justice.gc.ca  
Subject: Bill Bonner - Comments on Lawful Access Consultation Document



Comments on Lawful  
Access - Wor...

To Whom it may concern,

Attached, please find my comments on the Lawful Access Consultation document. It is a Word 2000 document.



## Comments on Lawful Access – Consultation Document

By



s.19(1)

Calgary Alberta

December 15, 2002



Thank you for opportunity to offer comments on the Lawful Access consultation document and for extending the submission deadline.

After reading the document I found myself unable to discern any clear rationale for considering these proposals that are aimed at increasing the ability to store, access and track information about Canadians and create criminals on the basis of potential, only. After searching many times, I am forced to conclude that the underlying motivation is the desire to meet the requirements of the Council of Europe's *Convention on Cyber-Crime*. I use the term desire deliberately as no other rationale is evident. I find this conclusion to be extremely disturbing and, as a consequence, I am not in favour of the proposals contained in this document. The need has not been established.

I tried to take some comfort from the statement on page five, that, "The government's approach recognizes the need for effective measures that balance the rights, privacy, safety, security and economic well-being of all Canadians." Unfortunately, the contents of the document fail to support that statement. The ability to achieve any sense of balance is rendered impossible through the *a priori* act of someone placing the *Convention on Cyber-Crime* on the scale and assigning it a weight and density greater than gold.

This critical assumption is subtly presented as a *fait accompli*, in a self-contained circular manner. Pieces of paper exist that someone has signed on behalf of Canadians. Apparently we are unable to live up to the pieces of paper without changing ourselves. Therefore, we must change ourselves to conform to their requirements. Everything begins and ends with these pieces of paper, without providing Canadians with a well-articulated and substantiated rationale to accommodate them. The *Convention on Cyber-Crime* has silently been granted an extraordinary status, an inviolable call to accommodate. This is unacceptable as it limits the scope of Canadian input. The *Convention on Cyber-Crime* itself should be the first part of the discussion.

The proposals outlined in the consultation document are challenges to the rights of Canadians and the expectation of freedom and privacy within Canada, free from unnecessary surveillance and intrusions. The onus for explanation to challenge that expectation, in this instance and in all others, lies entirely with those proposing such actions. They have the primary responsibility of articulating and presenting the best evidence and arguments of the risks and benefits of their proposals to Canadians, who then pass judgement on their perception of the validity of the arguments. This is a serious responsibility and if the party proposing exceptions fails to do this, then there is no basis on which to proceed.

The government has substituted the *Convention on Cyber-Crime* in place of the much more difficult (but minimal) requirement of providing an articulated basis and rationale for accepting the *Convention on Cyber-Crime* (The "Why are we considering this?" question) and, in the process, limits Canadian input to the managerial, "How are we going to do this?" question. The onus for clearly addressing the "Why are we considering conforming to the pieces of paper (the *Convention on Cyber-Crime*)?" has not been met and, therefore, consideration of these proposals is premature.

Evidence of the problems resulting from the failure to meet this minimum responsibility is reflected in some of the proposals highlighted below.

### **Who should pay?**

It is going to be very difficult to convince service providers to accept the costs of these proposals without clearly establishing and substantiating the need. In fact, assigning the costs to others for implementing surveillance capabilities may be one of the reasons that the minimum responsibility has not been undertaken. If it was even a remote possibility that the government would bear these costs, it is sincerely hoped that the government would demand that the costs, benefits, identification of alternatives considered and the basis for the particular proposals presented be established in a more substantial fashion than they are here. If the government would demand it, so too will others who are asked to pay the costs.

### **High expectations of privacy versus low expectations.**

Before we start talking about "high" and "low" expectations of privacy we must establish that these distinctions are meaningful to Canadians. I believe that privacy is the basic expectation unless there are compelling arguments made, in specific circumstances, to warrant an exception. Splitting the notion of privacy into gradations of privacy expectations ignores that basic expectation. For example, how can one possibly be secure in their person if it is arbitrarily decided that in all circumstances people have a low-privacy expectation with respect to their telephone numbers and addresses? Either or both of those items can be used to locate the person, which may be a threat to their security. Why would we accept exposure to potential threats without a clear rationale for risking the exposure? Who is making the distinction between types of privacy and why would the potential victim agree? Canadians should be the ones determining their privacy expectations and they may vary with the individual and the individual's circumstances. Arbitrary categorical distinctions deny Canadians this right, expectation and, in some cases, practical need.

### **Reasonable grounds**

Reasonable grounds, the only basis on which interception and search and seizure is warranted, is exactly what is missing in the consultation document. It has failed in its responsibility to argue reasonable grounds for putting the proposals forward. No reasonable grounds have been provided for considering them.

### **Court Orders**

I am not a lawyer and I found the discussion here rather confusing. The only comment I will offer is that if the request for surveillance cannot satisfy the courts then it should not be undertaken.

### **Interception of Email**

I found this section to be confusing as well and I thought unnecessarily so. To my way of thinking, the basic expectation is that communication is private and that the medium employed is not relevant. Communications of any kind should not be seized or intercepted without compelling reasons to do so. The standard for accessing email should be no different than the standard required for law enforcement to access written communications or tap telephones. It is not the medium employed that should be important, it is the expectation of the privacy of communications, with limited exceptions, and then only in specified circumstances and through legally sanctioned

s.19(1)

means. The *Convention on Cyber-Crime* may be making some distinctions, but since arguments have not been put forward on the risks and benefits of conforming to the *Convention on Cyber-Crime*, I find the discussion in the consultation document premature.

### Data Retention

It was not clear to me from the document that data retention legislation was not being considered. Various jurisdictions in Europe appear to have passed data retention legislation with the expectation that Internet Service Providers store data that passes through their servers. I strongly disagree with this idea.

It is my observation that stored data always attracts the attention of others. This includes the "studying" of Canadians (another form of surveillance), the potential for harassment and commercial exploitation, or forcing individuals to answer to the assumptions of others based on a view of the individual derived from the interpretation of limited data. I am not in favour of generating and storing data "just in case" or because it "might be useful." It is not worth creating and increasing the ability to track and monitor all Canadians for the faint hope that, someday, stored data on a handful of individuals "might" be useful. This is an example of folly of risk analysis, and attempts at minimizing the potential of risk, being carried to such an extreme that all Canadians are treated as potential criminals. It also makes a mockery of the concept of balance.

### Concluding Comments

The importance of the subject, challenges to the expectation of the right to be free from unwarranted surveillance and the expectation of privacy generally, dictates that those proposing exceptions to these expectations assume the onus of responsibility for substantially justifying their proposals. The *Convention on Cyber-Crime* does not qualify. The goal of striving for balance has meaning only if the best possible arguments for exceptions to those expectations are put forward, so that Canadians can assess them. I am willing to concede that there may be instances when exceptions are warranted, but only after Canadians are presented with a clear and complete analysis of the motivation and rationale. That has not been done here and the notion of balance under such circumstances has no meaning.

s.19(1)

s.19(1)

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 16 8:49 PM  
To: la-al@justice.gc.ca  
Subject: Comments on "Lawful Access -- Consultation Document"

Comments on "Lawful Access -- Consultation Document"  
<[http://www.canada.justice.gc.ca/en/cons/la\\_al](http://www.canada.justice.gc.ca/en/cons/la_al)>

[REDACTED]

General comments

=====

I realize the term "Lawful Access" is the accepted one, but in this context it seems to bias the discussion.

My understanding is that over the years, governments have learned the painful lesson that intelligence services must be separated from law enforcement agencies. Since 2002 September 11, this lesson seems to have been forgotten or ignored. The Consultation Document does not seem to reflect the importance of this separation: each question should be asked separately for each functional purpose.

Throughout the document, the term ISP is used as if it were meaningful. There are several functions that are lumped in this category, and the nature of the internet does not demand they be related. For example, my organization performs some of those functions and not others. And my organization is just a single family household.

The logic of certain parts of the document break down if there is no ISP. I would hope that the government would not forbid natural ways of organizing these functions just to make the internet fit into a regulatory regime.

Much of the document seems to presume that strong cryptography is an exception, not the rule. It is my belief that the internet should and will grow up to have strong encryption and authentication almost everywhere. In fact, I am working towards that end. See <<http://www.freeswan.org>>.

Much of the document seems to take accidental properties of existing telecommunications mechanisms and raises them to a more general right of law enforcement and security agencies. I do not recognize any such rights. More accurately, I do not recognize any such impingement on my rights. The first paragraph of the introduction of the Consultation Document is a particularly clear example of this.

Much of telecommunications interception has been based on opportunism: "because this is possible with the system, we should be able to exploit this". It is a large step to mandating a structure that enables such capability. I don't see any demonstration that this loss of rights is appropriate.

The Document ought to deal with the kind of access provided through

the backdoor of CRTC or other licensing. The proper mechanism for Lawful Access is special-purpose legislation, not a through a side-effect of regulation for other purposes.

The nature of the regulations contemplated is to reduce civil rights. That is serious business.

There is another effect: to reduce flexibility in the marketplace. The burden will reduce choices and increase the barriers to entry for businesses and consumers. An anti-competitive effect.

Introduction.  
=====

Just because it is possible to intercept telephone calls does not justify interception of internet communication.

According to the Solicitor General's Annual Report on the Use of Electronic Surveillance, the conviction rate is in excess of 90% in those cases where lawful interception evidence is used or adduced in court.

What percentage of lawful interceptions are used in court? In other words, how often are lawful interceptions in some sense justified?

Clearly, it is important to maintain the principle and powers of lawful access.

This document is about extending lawful access, not maintaining it.

The challenge is to do so in the face of rapid technological change and in a manner consistent with the Canadian Charter of Rights and Freedoms.

This seems to suggest that we should be extending this as far as the government can get away with, notwithstanding what is appropriate. Shame!

These rapidly evolving technologies pose a significant challenge to law enforcement and national security agencies that require lawful access to communications and information, as these technologies can make it more difficult to gather the information required to carry out effective investigations.

The word "require" is not at all justified here, and biases the whole discussion. Perhaps "would find useful" is more appropriate.

While providers of certain wireless services, such as Personal Communications Services, have since 1996 been required to have facilities capable of lawful access pursuant to a licensing obligation under the Radiocommunications Act, there are currently no similar obligations for other providers.

Providers of what? A strict reading would suggest "providers of wireless services". Clearly something much broader is meant, and should be stated and justified.

The technology used for Internet communication, the need for sophisticated equipment to lawfully intercept Internet communications and the lack of provisions that would require Internet service providers to implement procedures for lawful intercept capabilities, have created difficulties for investigators.



What is an ISP? Am I an ISP because I run my own mail server? DNS server? VPN? Am I an ISP because I can route packets through different broadband connections (my household has cable and ADSL broadband connections)? I would claim that none of the onerous regulations envisaged by this document should apply to me and yet they would be ineffective applied upstream.

I think this example shows that much of the Consultation Document is based on a shaky premise: that there is a large organization (the ISP) that can be regulated to effectively perform surveillance for police and security agencies. This does not reflect an intrinsic structure of the internet. Thank goodness.

To contribute to the development of this legal framework, and to help law enforcement and national security agencies navigate this new environment, partnerships with Canadian industry are more important than ever and must be consistently fostered and maintained.

Industry is an important stakeholder, but surely the citizen is even more important. The consultation document does not seem to recognize this beyond the inconvenience of the Charter.

This paragraph suggests Government coercing and conspiring with Industry against the citizens.

#### The Council of Europe Convention on Cyber-Crime =====

Canada has agreed to join this treaty through Bill C-36, the omnibus Anti-Terrorism Act. This is a travesty since much of what the treaty mandates is harsh acts to enforce "intellectual property" rights. Hardly a matter of terrorism.

The treaty itself is an example of what has been called "policy laundering". What (I hope) could not be passed as domestic legislation is brought in through the backdoor of a treaty.

The combination of these two makes me very concerned.

The public policy objectives of this process are to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada.

This is about extending Lawful Access, not maintaining it.

Surely extending civil rights, not just preserving them, should be a goal. Yet much of this document is about curtailing them.

#### LEGISLATIVE PROPOSALS =====

It is very hard to comment on this section since it seems to be based on the concept of an ISP, one that is not fundamental to the internet.

What is a "network termination point"? I think that I have a bunch inside my house. I don't want to give police or security agency access to my house through the contemplated legislation or regulations.

If service providers are mandated to provide Lawful Access, what capacity level (bandwidth) must they provide? Surely Lawful Access should be rare and hence a low bandwidth should be sufficient.

## Forbearance

=====

From the document, I don't understand the purpose of Forbearance. I certainly don't see how it would "avoid problems such as the creation of intercept safe-havens".

Arbitrary power in the hands of police and security services is dangerous. It can be used for making threats.

## Amendments to the Criminal Code and other statutes

=====

### Production orders

=====

However, except for a very narrow type of production/collection orders, there are currently no production orders provided for in the Criminal Code.

I would suggest these don't exist because they violate civil rights. Why should users of telecommunications lose rights that they have always enjoyed in Canada?

If production orders make sense, why limit them to telecommunications?

### General production orders

=====

I'm not sure that I understand what is being described. Is this casting a very wide net? In other words, the agencies could ask for everything, not just for documents of which they know the existence? "Fishing trips" are not generally condoned, and are not acceptable here.

### Specific production orders

=====

Except in these very limited cases, the current safeguard prevents important information from being gathered at an early investigation stage, even if there is a low expectation of privacy in relation to the information being sought.

Safeguards should not be lightly discarded.

the standard for Internet traffic data should be more in line with that required for telephone

Why should citizens accept such a lowered standard? I reject this presumption.

### Orders to obtain subscriber and/or service provider information

=====

There are many plausible business models where a service provider need not know the identity of the customer. I don't think we should effectively forbid these.

These are common in "the real world". Nobody knows if I buy Playboy.

However, if such conditions have not been met or if the custodian of the information is not cooperative, law enforcement agencies have no means to compel the production of information pertaining to the customer or subscriber without some form of court order.

This is probably a good thing.

A problem does exist in cases where no warrant can be obtained under the Criminal Code (e.g., s. 487) because law enforcement agencies may require the information for non-investigatory purposes (e.g., to locate next-of-kin in emergency situations) or because they are at the early stages of an investigation.

Two reasons are given:

- locate next-of-kin. There are other mechanisms to handle this. For example, communication to customer could alert him to an issue without revealing his identity. Mixing this up with law enforcement and security is just plain wrong.
- "non-investigatory purposes" ... "early stages of an investigation". This is clearly self-contradictory. Hardly a legitimate justification. These are exactly the things that are currently intentionally excluded.

#### Data-preservation orders

=====

It is not really clear to me what these would cover.

It is meant as a stop-gap measure to ensure that information vital to a particular investigation is not deleted before law enforcement officials can obtain a search warrant or production order.

...

what is a reasonable period for a custodian of data to be compelled to preserve data: 90, 120, 180 days?

Assuming such orders make sense, this range of time seem quite unreasonable. Surely something more like 48 hour makes sense. How could it take 120 days to get a search warrant? Perhaps only if one was not justifiable on day one?

#### Interception of e-mail

=====

However, some cases dealing with e-mails in Canada have taken the position that they are to be considered "private communications." For example, a judge in Alberta recently held that judicial authorization under Part VI was required to intercept e-mails since there was a reasonable expectation of privacy on the part of those sending and receiving them.

This seems like a good judgement. The rest of the section seeks to undermine this judgement. Shame!

#### Amendments to the Competition Act

=====

#### Access to Hidden Records

=====

This proposal involves the capability of requesting persons found on a search premises to provide any records hidden on their person, including hidden electronic and digital devices or media mentioned in the search warrant, to officers on the premises; and provide for an obstruction provision specific to those failing to comply.

I am not a lawyer, but it seems to me that this should only be legal if the person in question is arrested.

#### Other mechanisms to provide subscriber and service provider information =====

The shining example of the gun registration should serve as a warning. This is intrusive and expensive and needs more justification than is provided.

Law enforcement and national security agencies require accurate information on the subjects of their investigations in order to determine where to target an interception. Law enforcement agencies also require such information to obtain a search warrant.

The word "require" is rhetorically slippery. In some circumstances this information would allow them to target more investigations. It is not a general requirement.

Some states, such as Australia, the Netherlands and Germany, have established databases or statutory means for law enforcement and national security agencies to obtain accurate subscriber and service provider information more quickly. In these countries, telecommunications service providers are required to provide such information and are responsible for its accuracy, completeness and currency.

None of these countries have spotless civil rights records. For a very recent example of problems in the Netherlands, read:

<<http://www.fn1.nl/ct-nl/archief2003/ct2003-01-02/aftappen.htm>>

The implementation of such a database would presuppose that service providers are compelled to provide accurate and current information.

Compulsion is a serious matter.

Other options, including the use of existing sources of information such as provincial 911 databases or private telephone directories, may be appropriate. Any such option would need to be used in a way that is consistent with the Privacy Act, the Personal Information Protection and Electronic Documents Act, and any other applicable laws.

Information in these directories was collected for a different reason. It is a violation of the principles of privacy to use it for another purpose.

should an obligation to collect such CNA information be imposed even if the service provider does not collect this information for its own purposes? In other words, should a provider be compelled by law to collect CNA information?

No.

some mechanisms with respect to CNA information are already in place with respect to telephones. Should such mechanisms be created or adapted to provide similar subscriber information for Internet service

providers?

One does not justify the other. The question should be re-framed to reflect this. I would then answer "no".

Conclusion

=====

If my comments seem intemperate, it is because I find the presumptions of the document to be outrageous impingement of my civil rights.

Pierlot, Paul

s.19(1)

---

From: [REDACTED]

Sent: 2002 Dec 16 9:48 PM

To: la-al@justice.gc.ca

Cc: [REDACTED]

Subject: Lawful Access consultation

Please find attached comments of the Public Interest Advocacy Centre in response to the "Lawful Access" consultation.

s.19(1)

Pierlot, Paul

From: [REDACTED]  
Sent: 2002 Dec 16 11:30 PM  
To: la-al@justice.gc.ca; consultations@canada.justice.gc.ca

Greetings,

I have reviewed the Lawful Access consultation documents as posted on the Department of Justice website. I have attached a series of comments on the proposed legislative responses to the criteria layed out in the discussion paper.

I am a System Architect with [REDACTED] so I speak from the strengths of experience from the engineering perspective, and with the surety of watching the fallout of similar initiatives, like the Council of Europe's Convention on Cyber Crime.

#### 1) Intercept Capability

No legislation should be introduced that enforces a formal system of data interception points throughout the entirety of the Canadian electronic infrastructure. Such a system, by virtue of it's notion in relation to packet switched and cell switched networks, is vulnerable to abuse.

##### \* Requirement to provide interception capability

I am familiar with the technical architecture of the Canadian Internet backbone. In point of fact I was involved in implementing various autonomous systems which help comprise that backbone. Special requirements to provide intercept capability are not even technically necessary in the majority of cases. Intercept equipment often uses interfaces that are compatible with hardware present in most machine hosting facilities. Network equipment in many cases offers diagnostic capability which will facilitate lawful interception -- a condition which should define the exception, as opposed to the norm.

Additional requirements to provide explicit capability to intercept Internet traffic therefore do not appear to be necessary.

The following questions remain, however, even for current intercept equipment:

- A. Does intercept equipment remain connected indefinitely, and if so, through what means do providers gain assurance/proof that data is not being intercepted on an ongoing basis -- such as the case where Dutch intelligence turns out to have been leaking national secrets to Israeli intelligence through custom intercept equipment manufactured in Israel.. or in the more general case of system abuse by the intelligence community.
- B. What is the means in place to dissuade constant interception, once the technical deterrent of engineering a specific intercept point for each investigation has been removed? What possible response could offset abuse of such systems in the inevitable event of their abuse?

#### 2) Production, Anticipatory, and General Orders

Production orders are unnecessary, given the ability of law enforcement agencies to obtain information via existing means.

The rationale presented for the issuance of anticipatory orders is absurd.

"Should there be a specific power, parallel to that provided for in the Criminal Code dial number recorders, to allow law enforcement and national security agencies to obtain traffic data?"

Absolutely not. Why would the Canadian intelligence agencies be granted access to the data of Canadian citizens based on a model created for the investigation of criminal activities. Intelligence operations with respect to data networks are not target specific. They are ongoing, in a process best described in lay terms by drawing analogy to fishing with a large trawler and a very large net.

The mere possibility that 'traffic data' may constitute the actual content of a given network communication stream, underlines the substance of the force to overextend existing laws to leverage in new ones which impinge upon the Charter, pinching rights from the Canadian people. A dial number recorder is not a wiretap, however, a 'traffic data' intercept almost certainly is. No equality should be drawn between an intercept device capable of obtaining data from 'traffic' and a dial number recorder.

Under no current or foreseeable circumstances, should this power be enacted.

"Should there be a specific production order in relation to customer name and addresss and service provider information?"

Absolutely not. Warrants and court orders should be issued for this purpose. If law enforcement agents cannot convince a court to issue such warrants, this does not constitute a rationale to create new inherent powers. In point of fact, it should be a rationale not to. I am extremely concerned that a production order could be obtained where insufficient cause exists to believe that a specific criminal act has been committed.

Personal information must be protected unless a specific criminal act is being investigated. Any request by law enforcement is not itself a means to compel a person to provide personal information, unless that request is a component of a court proceeding or investigation empowered by the compulsion of the court.

### 3) Data-preservation orders

No data-preservation order should be issued without a warrant. The model presented suggests that such an order will be issued before a warrant is obtained. The obvious ramifications involve the increasingly large options for abuse, and the likelihood that such orders will be issued en masse, and without any kind of reasonable cause.

With regard to customer data collection, no telecommunications firm or internet service provider should be required, as a daily business practice, to compile what is essentially intelligence information on their user base. Especially where no crime is suspected and no specific individual is targeted for investigation.

### 4) Virus dissemination

The wording of this section, and the focus on 'virus' dissemination, is profoundly limited in both applicability and utility due to the following:



1. A significant number of mobile code threats are not 'viruses'
2. A significant threat is posed by code that is not mobile
3. System vendors are at least as culpable for selling systems needlessly prone to external code threats due to poor architecture and a failure to address such concerns, even for clients of the highest stature.
4. Such issues can be dealt with technically.

In general, when the political class attempts to codify 'cybercrime', the efforts have been disproportionately centred around 'virus' programs. This has always struck me, professionally, as misguided. I am certain that such a focus speaks to an insufficient depth of consultation with those within the system architecture, and information security field.

The problems with the limitations of this section are outlined below:

- A. Virus programs are not the only serious mobile code threat. There are many mobile, automated programs that exist which cannot be described as a 'virus' in the common use of that term. That this section is titled 'Virus Dissemination' concerns me, because it implies, rather myopically, that the existence of other threats have not been fully explored and understood.
- B. Mobile code is not the only serious threat. Some of the most serious security exposures I have seen over the last decade since the emergence of the modern internet, have nothing to do with mobile code or a 'virus' program. This reality, however, is entirely absent from the discussion presented in the lawful access documentation, raising the concern that insufficient consultation with the security community has been conducted within Canada prior to creation of this proposal. Just two examples (quite famous in technical circles) include the suite of SNMP vulnerabilities discovered in early 2002 and the distributed denial of service attacks which gained broad media coverage in Feb. 2000, which themselves largely begat the furor over security to which your paper is largely a response.
- C. Remedies which target virus authors/users alone necessarily target a very limited proportion of the intruder community, because the creation of viral mobile code, while not unknown, is exceedingly rare within the highly skilled component of the intruder community. In point of fact, most of the systems that attract the attention of such people aren't prone to infection of viral mobile code at all. Given that the systems which manage nameservice, routing, webservice, and mail for a large majority of the top commercial organisations in the world fall into this class, the provision comes as a red herring. A federal order to prevent government from purchasing Microsoft operating environments for mission critical applications would go a tremendously long way to eliminating any requirement for this provision to begin with.
- D. Some attacks require no tools at all, so the "Virus Dissemination" provision will provide no reasonable assistance when prosecuting so-called 'insider' attacks, or 'social engineering' attacks where no special software is required to successfully cause high-dollar operational disruption.

My specific responses to statements and legislative options are as follows:

"Under the current provisions of the Criminal Code, only the effects of spreading a computer virus, or an attempt to do so, are criminal acts."

The Criminal Code should NOT be modified from this wording. It is my opinion as a security professional that changing the wording of

the Code will in this instance not result in a reduction of risk, but instead only jeopardize valuable, legitimate security research.

"The Council of Europe Convention on Cyber-Crime requires signatory states to criminalize the creation, sale and possession without right of devices (e.g., computer programs) that are designed or primarily adapted for the purpose of committing offences specified in the Convention, whether or not the virus has been deployed or has caused any form of mischief."

There are many serious problems inherent in the Council of Europe Convention on Cyber Crime; extrapolating from that flawed convention to specific acts in law, in Canada, is potentially extremely dangerous to the evolution of the high technology economy, and Canada's competitiveness among its peers in the first world. Software programs are a form of speech. I do not believe Canada should ratify any agreement that criminalizes speech in any form, for all the reasons outlined in the Charter, and because it will have no meaningful effect in reducing risk.

All of the Charter-related speech issues aside, the issues I have with the rationale presented are as follows:

- A. Every information security professional involved with assessments and testing possesses software applications which fit the description of a criminal device above. Every security researcher who develops a proof-of-concept computer program to demonstrate security exposures would be similarly guilty of a criminal offense. In many cases, these software applications are the EXACT applications used by criminals. There will be no means of differentiating between a "legitimate" tool and a "criminal" tool by physically examining program object or source code should that be available.
- B. Creating new criminal acts does not arrest and convict people; law enforcement does. Both federal and provincial law enforcement groups lack adequate resources for investigating and prosecuting computer crime. Until this situation is corrected, criminalizing entire genres of software applications will do nothing to aid in the actual prosecution of criminal acts or deter those who would commit them. Such criminalisation would, however, castrate the private security intelligence community and hamper research into system security secure system architecture, and pure research in the mathematics of encryption.

In summary, in my professional opinion:

1. Council of Europe provisions for criminalisation of software is wrong headed and in direct opposition to Charter protections of free expression.
2. Criminalization will not address most of the most serious security threats
3. Criminalization will seriously impact the security community
4. Criminalization will chill legitimate and important research
5. Police resources are insufficient to enforce even existing laws
6. Criminalization will not reduce the threat to Canadian systems

Do not alter the Criminal Code in this fashion. Do not ratify the Council of Europe Convention (a piece of law unparalleled in its flaws since the American DMCA), particularly if it requires such Criminal Code alterations. Please consult members of the information security and architecture communities directly if further discussion of software criminalisation is required.

- 5) Interception of e-mail

There should be absolutely no differentiation between the postal mail system in this country and the use of e-mail to issue communications. At every step where postal mail would be considered a private communication, an e-mail message should also be considered a private communication.

Any specific proposal for the interception of e-mail must make very clear reference to the stages of the email delivery process to make certain that the essence of private communication protection has been properly upheld.

#### 6) Service Provider Information

"what type of mechanism, if any, should be put in place to provide law enforcement and national security agencies with up-to-date and accurate CNA and LSPID information while respecting the privacy of Canadians?"

Personal information which belongs to Canadians should not be provided to agencies when there is no reasonable likelihood of a legal proceeding. CNA, like any information which links a name to a number and physical location, is protected personal information.

"should an obligation to collect such CNA information be imposed even if the service provider does not collect this information for its own purposes? In other words, should a provider be compelled by law to collect CNA information?"

No. Companies should not be forced to request personal information they do not require for business purposes simply to provide it to RCMP and CSIS. The Government of Canada should in fact attempt to better protect Canadians from unnecessary requests for personal information.

The Government of Canada must cover all costs associated with a new CNA collection effort.

No police or security agency should operate this database directly.

Thank you for your consideration of these responses. It is my sincere hope that the Government of Canada will carefully weigh any perceived benefit of these proposals with the potential for serious impact, not only to the integrity of the telecommunications industry, the internet industry, and the information security industry, but also to the vital civil liberties of all Canadians -- the set of conditions that make being Canadian the best of all outcomes, for any person.

Should you have any questions, or require further comment, I would be happy to oblige.

Yours sincerely,

s.19(1)

DeepSky Systems <http://www.deepsky.com/>

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 17 2:23 AM  
To: la-al@justice.gc.ca  
Subject: Vancouver Community Network's Comments Regarding the Proposed Lawful Access Legislation

[Due to a delay in completing these comments, they are being forwarded in plain text. A signed copy on VCN's letterhead will be provided in due course.]

I am writing on behalf of the Board of Directors of the Vancouver Community Network (VCN), a regional freenet and registered charity which provides email accounts, web site space, dial-up access, training courses, and other online services to the public in the Vancouver region. Two of VCN's most important purposes are to provide internet access for low income people who cannot afford commercial services, and to provide web site space and other services for hundreds of groups which serve the Vancouver community.

#### Introduction

On September 30, 2002 the Board of Directors of the Vancouver Community Network passed a resolution "that VCN express our strong disagreement with the [lawful access] proposal". Below are a number of reasons why VCN believes that the proposal is an unjustified and unacceptable violation of the fundamental interests of our users, staff and volunteers.

First, there is no need for any increased police powers in regard to Canadians' use of the internet. Existing laws provide ample authority to investigate criminal use of the internet when the police are able to satisfy a judge that there is probable cause for doing so.

Second, allowing the police to intercept messages or obtain personal records in the absence of such probable cause would effectively destroy Canadians' right to privacy in browsing, email, and other online activities that are increasingly essential to their everyday life.

Third, the proposals would violate the rights of i.s.p. staff by forcing them to participate in spying on their customers and users. This would be an especially offensive requirement for non-profit organizations like VCN which rely heavily on dedicated volunteers to perform many important administrative and technical tasks.

Fourth, the increased costs for equipment, software, and staff or volunteer time would detract from the ability of VCN to provide the services our users need and want. This, combined with the loss of trust that would result from users' knowing that VCN may turn over copies of their internet logs and email, could jeopardize our survival, which depends heavily on voluntary contributions by our members.

Finally, the proposal would seriously hamper the ability of non-profit groups which provide information and advice regarding legal, health, family planning and other sensitive and confidential matters, to continue using the internet to communicate with those who need their services.

Most of these matters are ably addressed in the submissions of Telecommunications Canada and the Freedom of Information and Privacy Association, which we fully endorse.

We will elaborate briefly on certain points that are of special

significance to VCN and the community groups and individuals who rely on our services.

### Impact on Staff and Volunteers

There are three aspects to this concern. First, neither our paid staff nor our dedicated volunteers joined VCN in order to spy on their friends and neighbours. The parts of the proposal that could require them to actively participate in police investigations by maintaining and turning over confidential records would be highly offensive to them. We suspect that many staff of commercial service providers would be equally offended, but at least in some commercial situations the employer has the resources to hire special security staff so that the regular employees who serve the public would not be required to take part in the process. VCN and other freenets would not have that luxury.

Second, the time that would be required to institute new record-keeping procedures and install and maintain whatever new hardware and software may be required would necessarily be taken from the available time to serve our members. Staff and volunteers only have so much time, and no one is going to voluntarily work overtime to help the police violate users' rights. If, as we suspect, some of our staff and most of our volunteers refuse to cooperate at all with such demands, the impact on our remaining staff and their regular work will be great.

Third, the existence of such records will be a magnet for hackers who want to embarrass their enemies, employers or employees, or family members by finding out what they were doing on the internet over the last several months. The cost of the proposal would therefore have to include the time to plan and implement the most rigorous possible security measures to protect the data from illegitimate internal and external access.

### Interception of Confidential Communications from Third Parties

One of VCN's most important services is to provide space and services for thousands of non-profit "community information providers" to maintain web sites, email lists, and tools that enable them to better serve the public. Some of these community groups engage in legal, health, family or crisis counselling, which involves discussion of highly sensitive and personal matters via individual email and group email lists. For example, PovNet maintains confidential email lists that enable lawyers and community advocates to consult with each other about difficult cases, law reform issues, and other sensitive matters. Like s. 488.1 of the Criminal Code, which was struck down by the Supreme Court of Canada as a violation of s. 8 of the Charter because of its impact on solicitor client privilege, the lawful access proposal would violate the privacy of advocates and others who use the internet.

Moreover, because of the nature of email and email lists, the violation could not be limited to just the individual who is the subject of an investigation. If such a person were a member of a confidential list, every message posted to the list would be sent to the person's inbox and thereby be included in the records to be accessed. The vast majority of these messages would have nothing whatever to do with the target, but all of them would end up in the hands of the authorities under the proposed measures. No technological measure would be possible to prevent this, or to allow the third parties to protest the disclosure. The interception of telephone conversations poses no similar danger. This suggests that legal protections for email interceptions must be at equal to those for telephone wiretaps, if not greater.

### Conclusion

If there were an apt analogy to these outrageous proposals, it would be a requirement that the staff of Canada Post open and copy every piece of

mail they process, so that the contents will not be "lost" if the police should later decide that the letters might be evidence of criminal activity. No sane government would dare make such a suggestion, however useful it might sometimes be to have copies of a suspect's mail. Why should the wholesale violation of Canadians' privacy for the convenience of inquisitive authorities be considered any more acceptable just because it concerns email and the internet?

The internet may be relatively new, but the fundamental values of privacy and civil liberties have not changed. Our rights were won and preserved by the sacrifice of earlier generations, often in the face of threats far greater than anything that exists today. Respect for them, and for the country they have left us, makes it unthinkable that we should surrender those rights now, whether on the pretext of fighting terrorism, or of imitating a bad European or American law.

--

Community Legal Assistance Society

s.19(1)

Per: [REDACTED]

Suite 800, 1281 West Georgia Street

Vancouver, B.C. V6E 3J7

Tel: (604) 685-3425 (68-LEGAL)

Fax: (604) 685-7611

E-Mail: [REDACTED]

Pierlot, Paul

From: [REDACTED] s.19(1)  
Sent: 2002 Dec 17 11:33 AM  
To: la-al@justice.gc.ca  
Subject: REVISED Submission on Lawful Access



PIAC-Dec16-02.doc

Late yesterday, we submitted comments on the Lawful Access consultation, from the email address "pl.lp@cyberus.ca". Attached, please find a REVISED version of those comments, correcting some formatting and typographical errors for which we apologize. Please replace the version sent yesterday with the attached.

Thank you,

[REDACTED]  
Public Interest Advocacy Centre  
1204 - 1 Nicholas St.  
Ottawa, Ontario, Canada K1N 7B7  
tel: 613-562-4002 x.24  
fax: 613-562-0007  
email: [REDACTED]  
PIAC website: <http://www.piac.ca>

# Public Interest Advocacy Centre

## Comments on the Federal Government's "Lawful Access" Consultation Document

December 16, 2002

CONTACT:

s.19(1)

  
1204 – 1 Nicholas St.  
Ottawa, ON K1N 7B7  
(613) 562-4002 x.24

  
<http://www.piac.ca>



## Table of Contents

INTRODUCTION.....	3
GUIDING PRINCIPLES .....	3
GENERAL CONCLUSIONS .....	4
LACK OF SUPPORTING DATA .....	5
TECHNICAL OR LEGAL PROBLEMS? .....	5
TECHNOLOGICAL NEUTRALITY.....	5
MAINTAINING LAWFUL ACCESS CAPABILITY VS. INCREASING LAWFUL ACCESS CAPABILITY ...	6
THE COUNCIL OF EUROPE CONVENTION ON CYBER-CRIME .....	6
LACK OF CORRESPONDING PRIVACY SAFEGUARDS .....	7
INTERCEPT CAPABILITY .....	8
EMAIL INTERCEPTION .....	10
REASONABLE EXPECTATION OF PRIVACY.....	10
INTERCEPTION OR SEARCH AND SEIZURE?.....	10
ACCESS TO SUBSCRIBER AND SERVICE PROVIDER ID .....	10
DEFINITIONS .....	10
OTHER MECHANISMS TO PROVIDE SUBSCRIBER AND SERVICE PROVIDER INFORMATION.....	13
PRODUCTION ORDERS.....	13
GENERAL PRODUCTION ORDERS .....	14
PRODUCTION ORDERS FOR "TRAFFIC DATA" .....	14
PRESERVATION ORDERS .....	15
VIRUS DISSEMINATION .....	16
EXTRA-TERRITORIALITY.....	17
CONCLUSION .....	17

## Introduction

The Public Interest Advocacy Centre (PIAC) is a national non-profit organization devoted to the representation of consumer interests in matters involving public utilities, essential services, and public interest issues of broad application to Canadians. PIAC has developed a strong record of consumer advocacy since its inception in 1976, and is widely recognized as an important and influential voice for ordinary consumers in a variety of marketplace issues. Over the past decade, PIAC has become a leading advocate of consumer privacy interests, in the context, especially, of the electronic marketplace. PIAC is governed by a distinguished volunteer Board of Directors from across the country, and is supported by member groups and donors representing hundreds of thousands of Canadians.<sup>1</sup>

PIAC is grateful for the opportunity to comment on the important issues raised in the Consultation Document issued August 25, 2002 by the Government of Canada on "Lawful Access". We commend the Government on its efforts to reach out to, and obtain input from, civil society through advance consultations on these issues. However, our ability to provide feedback is limited due to a lack of detail and clarity regarding the legislative proposals as well as the problems they are designed to overcome. Our comments below are therefore more general than might otherwise have been the case.

We look forward to an opportunity to review and comment on more specific legislative proposals accompanied by more substantial evidence as to their need.

## Guiding Principles

The guiding principles for lawful access in Canada have already been established in the *Canadian Charter of Rights and Freedoms*, and Supreme Court jurisprudence interpreting these fundamental rights and freedoms. Under section 8 of the *Charter*, "everyone has the right to the secure against unreasonable search and seizure", "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society". A significant body of jurisprudence has developed under this principle, providing helpful guidance as to where the line is to be drawn between reasonable and unreasonable intrusions by the state into the personal lives of individuals.

The Supreme Court of Canada has repeatedly confirmed the importance of privacy as an essential aspect of an individual's liberty in a free and democratic society.<sup>2</sup> As noted by the Court,

<sup>1</sup> For more information, see <http://www.piac.ca>

<sup>2</sup> E.g., *R. v. O'Connor* [1995]; *R. v. Duarte* [1990]; *R. v. Dyment* [1998].

## PIAC Lawful Access Consultation Submission

"The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communication will remain private."<sup>3</sup>

The Court has also emphasized the importance of prior judicial authorization as an essential safeguard against undue invasion of individual privacy by the state:

"The state's interest in detecting and preventing crime begins to prevail over the individual's interest in being left alone at the point where credibly-based probability replaces suspicion. History has confirmed the appropriateness of this requirement as the threshold for subordinating the expectation of privacy to the needs of law enforcement."<sup>4</sup>

In *R. v. Oakes*,<sup>5</sup> the Court established a clear test for the determination of whether a given infringement of *Charter* rights is reasonable and demonstrably justified. This test requires a sufficiently important objective served by the infringement, a rational connection between the means and the ends, and minimal impairment of the right in question.

We agree with the Privacy Commissioner of Canada that any new privacy-invasive measure that purports to enhance security must meet the following test:

- it must be demonstrably necessary in order to meet some specific need;
- it must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer;
- the intrusion on privacy must be proportional to the security benefit to be derived; and
- it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose.<sup>6</sup>

## General Conclusions

Having reviewed the Consultation Document, and participated in a day-long consultation with government officials, it is PIAC's view that the Government's proposals for greater lawful access to private communications have not been demonstrably justified, according to the test articulated by both the Supreme Court of Canada and the Privacy Commissioner of Canada. In particular,

- it is not clear that greater access by law enforcement to electronic communications will in fact, or is even likely to, increase the security of Canadians;

<sup>3</sup> *R. v. Duarte* [1990] 1 S.C.R. 30, at para 24.

<sup>4</sup> *Hunter v. Southam*, [1984] 2 S.C.R. 145 at 166-7.

<sup>5</sup> [1986] 1 S.C.R. 103.

<sup>6</sup> Comments, November 25, 2002.

- the privacy intrusions that would result from these proposals are clearly significant, while the security benefit to be derived therefrom is unclear;
- it has not been demonstrated that no other, less privacy-intrusive, measure (e.g., focused on technological and/or administrative impediments) would suffice to achieve the same purpose of enhanced security.

We fully appreciate the need for law enforcement agencies to be able to protect citizens against criminal activity without undue effort. We are as interested as everyone in the security and safety of Canadians. However, we strongly oppose measures that provide law enforcement agencies with greater powers of intrusion into the private lives of individuals, without adequate safeguards against the abuse of such powers.

### ***Lack of Supporting Data***

The legislative reforms being considered are premised on a need for enhanced state power in the face of technological change and specific barriers that exist today. Yet, the government has provided little evidence to justify the significant privacy intrusions posed by increased lawful access. Without specific information as to the extent and nature of the problem(s) to be rectified, it is impossible to conduct the "cost/benefit" analysis required by the Supreme Court.

Indeed, PIAC is unable to answer most of the specific questions posed in the Consultation Document because of the lack of information provided to justify the proposals.

If evidence is available to justify the proposed measures, it should be made public, so that Canadians can weigh it and thus make informed judgements as to whether the security benefits of the measures outweighs the privacy costs. If such evidence does not exist, then there is no case for the measures in question, and they should be dropped.

### ***Technical or Legal Problems?***

The Consultation Document identifies a number of technological developments that have created problems for law enforcement investigations (p.4). It would appear that the problems in question are technical, rather than legal. If law enforcement agencies have difficulty dealing with new technologies of communication, the solution is not to lower the legal standard for interception or search and seizure; rather, it is to provide law enforcement agencies with the technical expertise they need to deal with the evolving environment.

### ***Technological Neutrality***

The proposals would effectively establish a lower standard for interception and/or search and seizure in the online context, versus in the offline context. Yet, no justification in principle has been provided applying a different standard depending on the mode of communication used.

PIAC submits that legal standards should not differ according to technology. Not only would this be unprincipled; it would lead to a situation in which the government is constantly playing legislative "catch up" with new technologies. Criminal Code standards should be designed to apply regardless of technology, and legislative reform should focus on ensuring that the standards in question are worded so as to incorporate all relevant technologies (rather than on establishing lower standards for certain types of technology).

### **Maintaining Lawful Access Capability vs. Increasing Lawful Access Capability**

The Consultation Document states that the objective of the Lawful Access proposals is "to maintain lawful access capabilities for law enforcement and national security agencies in the face of new technologies".<sup>7</sup> Yet, the proposals go much further than *maintaining* existing lawful access capabilities – instead, they would significantly *increase* the ability of law enforcement and national security agencies to intercept, search and seize electronic communications of individuals, and personal information about individuals in electronic form.

PIAC has no objection to updating Canadian legislation so that the well-established Canadian standards of lawful access to private communications and personal data are clearly applicable in the context of new communications technologies. We do, however, object to a substantial weakening of such well-established safeguards.

### **The Council of Europe Convention on Cyber-Crime**

It is unclear to what extent the proposals in question have been driven by forces outside Canada. According to the Consultation Document, the Council of Europe *Convention on Cyber-Crime* requires that ratifying countries provide in their domestic law for Production Orders, Preservation Orders, and an offence in relation to computer viruses that are not yet deployed.<sup>8</sup> PIAC's comments on these specific proposals are set out below.

In general, however, we are concerned that some aspects of this *Convention* may be inconsistent with Canadian values, insofar as it requires provision for an unreasonable level of state incursion into the private lives of individuals, without adequate privacy safeguards. In our view, Canada should not ratify the *Convention* if to do so would be inconsistent with Canadian values and rights as set out in our *Charter of Rights and Freedoms* and interpreted by the Supreme Court of Canada.

### **What position did Canada take in the negotiations?**

There is absolutely no information available as to the position that Canada took in the negotiations. If this information were available, it would aid in understanding and framing the lawful access proposals.

---

<sup>7</sup> p.6.

<sup>8</sup> p.5.

### **What are the options being considered (and not considered)?**

Similarly, no information is available to understand which options were considered and rejected in the process leading to the convention signing. Why was there no pre-signing consultation to review and direct the position that Canada would take?

### ***Lack of Corresponding Privacy Safeguards***

While clearly aware of privacy concerns, the government does not appear to have made a serious attempt to weigh them against the pressure from law enforcement agencies for easier access to personal information in the electronic environment.

### **Privacy, as much as national security, is under attack**

The same technologies that law enforcement agencies complain are hindering their ability to investigate criminal activities, have also provided the basis for an unprecedented erosion of individual privacy. Individual privacy is increasingly under assault by virtue of the vastly easier access to vastly greater quantities of personal information available electronically. We find it particularly ironic in this context that the government seeks to further erode individual privacy, in the name of the public interest. If anything, privacy protections for electronic communication should be stronger than for non-electronic communications, given the unprecedented opportunities that electronic technologies offer for surveillance and intrusion.

### **The Need for Privacy Safeguards**

In contrast to the Lawful Access legislative proposals, is the government's recent legislative initiative on Money Laundering (*The Proceeds of Crime Act*). Just over two years ago, the federal government consulted with the Privacy Commissioner and the public on legislation designed to detect and deter money laundering and to facilitate the investigation and prosecution of money laundering offences. In response to concerns raised by the Privacy Commissioner and stakeholders, the government included a number of measures designed to limit otherwise enormous systemic individual privacy invasions that would have been authorized. For example, Bill C-22 (as it then was) included provisions:

- exempting lawyers from the requirement to disclose communications, where such communications are subject to solicitor-client privilege;
- requiring the police to obtain a judicial warrant in order to obtain detailed information from the new Financial Transactions and Reports Analysis Centre of Canada (FTRAC);
- limiting the use of information by FTRAC or other officials to purposes of exercising powers or performing duties and functions under the Act;
- making a punishable offence the improper disclosure of information; and
- giving the Privacy Commission oversight powers in relation to FTRAC's handling of personal information.

In contrast, the Lawful Access proposals contain no safeguards against abuse of the increased powers they would provide.

## PIAC Lawful Access Consultation Submission

### Recommended Safeguards

The proposal assumes almost unlimited levels of citizen trust in law enforcement and national security agencies; trust that historically has not always been deserved. It argues for the need to infringe upon individual rights, suggesting this will enhance collective public security. As noted above, PIAC does not consider that the proposals have been adequately justified.

Should they nevertheless proceed, any proposals for greater access by law enforcement agencies to private communications and information must be accompanied by strong oversight mechanisms that ensure public accountability, transparency and scrutiny. This oversight should require routine reporting on measures undertaken in the name of law enforcement and national security and an accounting of the efficacy of these measures. Such reporting would enhance public confidence in the government and its agents exercising their rights to intercept and collect personal data.

Specific and severe penalties for improper use or disclosure of personal data collected via lawful access, as well as for improper attempts to access personal data, should be introduced

Specific procedures should be enacted for the destruction of information seized or acquired as part of a lawful access endeavour, at a minimum these should include:

- Specific guidelines to be followed for destruction
- Specific guidelines to be followed to notify parties whose information has been intercepted

Specific procedures should be enacted for the handling of intercepted or seized information that is subject to legal privilege.

In summary, we believe that all interception and/or search and seizure of electronic communications should require judicial approval, should identify a specific target, should identify specific information to be seized/intercepted and should have a specific rationale and justification for the seizure or interception. We also believe that any orders issued should be time-limited.

### Intercept Capability

The government is proposing to introduce a general requirement in legislation to ensure intercept capability, with the specific details to be contained in regulations proclaimed at the time the legislation will come into force. It is proposed that all service providers (wireless, wireline and Internet) be required to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies.

We recognize that there may be a need for assurance, on the part of law enforcement agencies, of the ability to intercept and monitor electronic communications upon the issuing of judicial authorization. However, the government has failed to present evidence that the deployment of this massive surveillance infrastructure is necessary. For example, we do not know how many investigations have been thwarted as a result of the lack of technical capability. Moreover, the lack of clarity regarding evidentiary thresholds, oversight and safeguards makes us unable to provide an opinion on this proposal.

The Consultation Document suggests that many of the important details of such interception capability requirement (e.g., cost recovery) would be left to regulation. It is important that any regulations be subject to full public review. We echo the call from CWTA and CAIP and request that the draft legislation and accompanying regulations be made available for a full and complete public review, and that sufficient time be provided for interested parties to assess their impact and submit comments.

### **Effect on future innovation and adoption of technology**

It is possible that impact the proposed requirement for intercept capability will have an adverse effect on future innovation in this industry. In particular, if intercept requirements are not applied to current infrastructure but only "when a significant upgrade is made to their systems or networks",<sup>9</sup> ISPs may be disinclined to upgrade their operations or capabilities. This could limit innovation and is therefore arguably in conflict with Canadian telecommunications policy.<sup>10</sup>

### **Cost implications**

We are concerned that the cost of constructing the surveillance infrastructure may unnecessarily burden the industry, and hence the telecommunications user. This, again, is arguably in conflict with Canadian telecommunications policy.<sup>11</sup> In any case, it is impossible for us to address this issue fully without more information as to the costs in question.

It is certain that there will be disagreement between the industry groups and others with respect to costs. Some have envisioned the ISPs assuming the costs of 'lawful access', others have envisioned the government providing funding through some form of authorized tariff. Either way, it is clear that the citizen, as a telecommunications user or as a taxpayer, will be responsible for the costs of 'lawful access'. Any such costs should be minimized.

---

<sup>9</sup> Consultation Document – Pg. 10.

<sup>10</sup> Section 7 (g) - *Telecommunications Act* - STATUTES OF CANADA, Chapter 38.

<sup>11</sup> *Ibid.*, Section 7 (a-h).



## **Email Interception**

The government seeks input on whether, or when, email constitutes a communication subject to interception, or instead a document subject to search and seizure. Different standards for access apply, depending on which approach is taken.

### ***Reasonable expectation of privacy***

Canadians have come to expect a high degree of privacy in email, despite widespread awareness of the ease with which such communications can be accessed by third parties. Increasingly, we are using email to communicate highly sensitive information, and indeed are relying on it to the same extent that we rely on postal mail. Canadians have, we submit, a similar reasonable expectation of privacy in email as they do in other forms of communication.

However, it is important to recognize the limits of the "reasonable expectation" test, where rapidly developing technology is concerned. Internet and email communications is an area in which technology and business practices have far outpaced the law. As a result, "reasonable expectations" may be based not on what is *desirable*, but rather on what we *know* to be the case, as undesirable as it may be. The legal treatment of email should not be determined by technological capability, but rather by our values as a society. If we wish to be able to communicate privately by email, without the possibility of unjustified surveillance, we should construct our laws so as to protect that desire. Principle, not technology, should guide our determination of this issue, as it did in the context of cellular telephone privacy.

Proceeding on this basis, PIAC submits that the Criminal Code should be amended to clarify that email, at least while in transit, constitutes a "private communication" under s.183. It would then be subject to the same procedural safeguards as all other interceptions under this provision.

### ***Interception or Search and Seizure?***

While in transit, interception of email is clearly just that: interception. It is a good question, though, at what point in the process of communication/delivery email is no longer a communication subject to interception, and is instead a document subject to search and seizure. The Criminal Code should be clear about when and where the line is to be drawn, if at all, between these two possibilities.

## **Access to Subscriber and Service Provider ID**

### ***Definitions***

CNA = Customer Name and Address (in effect the identity of the subscriber).

LSPID = Local Service Provider Identification (identifies the company that provides services to the subscriber).

The government's consultation document states that, "Basic customer information such as name, billing address, phone number and name of service provider, has historically been made available by service providers without a prior judicial authorization (such as a search warrant)."<sup>12</sup> Recent changes in the telecommunications sector, however, have left law enforcement agencies with a patchwork of differing and inconsistent policies among service providers, regarding the provision of this information upon request. The *PIPED Act*, for its part, permits (but notably does not require) private organizations to disclose this information upon request by law enforcement officials without judicial authorization. Instead, it is left to the government to determine what limits, if any, should apply in respect of access by law enforcement agencies to this information.

Notwithstanding the discretion afforded service providers by virtue of PIPEDA, we believe that from a public policy perspective, it is beneficial to build a clear, consistent, privacy-protective policy framework that balances all of the competing interests.

### LSPID

The CRTC recently ruled on the LSPID issue in the context of telephone service providers, requiring that, in order to obtain this information from Bell Canada, a law enforcement agency (LEA) must identify its lawful authority to obtain the information, and indicate that:

- (i) it has reasonable grounds to suspect that the information relates to national security, the defence of Canada, or the conduct of international affairs;
- (ii) the disclosure is requested for the purpose of administering or enforcing any law of Canada, a province, or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing or administering any such law; or
- (iii) it needs the information because of an emergency that threatens the life, health or security of an individual, or the LEA otherwise needs the information to fulfill its obligations to ensure the safety and security of individuals and property.<sup>13</sup>

PIAC submits that the CRTC test for LSPID disclosure by Bell Canada is appropriate, and should be adopted in respect of other communications service providers.

### CNA

On the other hand, we believe that access to CNA data should require judicial authorization. Customer name and address information can be sensitive information, depending on the context. It is not clear why we should grant law enforcement agencies unimpeded access to this information. Clearly, much of this information is already easily accessible in the marketplace, through published directories. However, many subscribers choose to protect their privacy by not publishing their contact information; in these cases, at least, individuals have a high expectation

<sup>12</sup> Consultation Document – Pg. 12.

<sup>13</sup> Telecom Decision CRTC 2002-21, 12 April 2002, para.22.

PIAC Lawful Access Consultation Submission

of privacy regarding their contact information, and such expectations should be reflected in the standard applied for lawful access.

With respect to Internet address information, we strongly object to a lower standard of access given that the ability to link such information to identified individuals would permit the collection of a vast amount of personal information.

Some may argue that by requiring judicial authorization for CNA release, we will create a system that is expensive, inconvenient and unfairly burdens the law enforcement or national security agency. We submit that these are not the only factors to consider when drafting public policy. Rather, it is imperative in a free and democratic society to balance the legitimate needs of the state with appropriate roadblocks to protect the rights of the citizenry from incursion by the state; this may, in fact, be expensive and inconvenient and may burden the state. Freedom has a cost; we believe the state can more properly bear the burden of this cost.

**Obligation to collect where none exists**

We have been asked to comment on whether the obligation should be imposed on service providers to collect this information in circumstances where they are not currently collecting this information for their own purposes. This obligation would likely affect those service providers and retailers selling prepaid and other anonymous telephone cards and phones.

We would imagine, for this to be implemented, a customer would need to present approved identification to a retail clerk (e.g. a convenience store clerk) who would verify and copy down the identification; this would then be forwarded to the service provider. This would be a gross invasion of privacy<sup>14</sup> and present even greater opportunities for data leakage or loss (and subsequent threats such as identity theft).

In discussing this point, we are struck by the fact that this proposal appears to conflict with the implicit premise of the consultation as attempting to overcome differences in legal process necessitated by technology. For example, if we require name and address to be supplied by persons purchasing pre-paid cards and anonymous wireless phones; why are we not similarly requiring persons utilizing the services of Canada Post to identify themselves? Should we not seal all Canada Post street mailboxes and require people depositing mail to present themselves at a government approved post office and present their government approved identification to a government approved counter clerk? Most correspondents would recognize the lunacy and Orwellian effect of such an unprecedented level of state intrusion.

We should not afford any lesser protection, or impose any higher burden on service providers, retailers and end users merely because they wish to avail themselves of technology solutions as an alternative to Canada Post.

<sup>14</sup> *Comments of the Privacy Commissioner of Canada on Lawful Access*, November 25<sup>th</sup>, 2002.

## ***Other mechanisms to provide subscriber and service provider information***

The government raises the topic of 'other mechanisms' for law enforcement and national security agencies to access subscriber (CNA) and service provider (LSPID) information, arguing that, "the only way in which this information can be obtained is through the time-consuming and costly process of directly contacting each local carrier."<sup>15</sup> The Canadian Association of Chiefs of Police has suggested the concept of a national database be constructed containing CNA and LSPID information for 'lawful access' use.

We recognize that it is not always an easy task for law enforcement and national security agencies to obtain CNA and LSPID information. We recognize that considerable cost and effort may be expended to locate this information. However, we believe that these are not the only factors to consider when drafting public policy. Creation of a national database of any personal information, even limited to CNA information, raises the potential for misuse and should therefore be avoided.

## **Production Orders**

In keeping with requirements under the Council of Europe *Convention on Cyber-Crime*, the Government proposes to create a new type of authorization for lawful access to documents held by a private body. A "production order" would require the custodian of documents to deliver or make available the documents within a specified period.<sup>16</sup>

The concept of production orders raises concerns about forcing private service providers into a role of agents of the state. It is at least questionable whether such "conscription" of third parties to carry out law enforcement activities is appropriate. It would undoubtedly interfere with the primary role of serving customers, and would effectively expand the reach of law enforcement well beyond current limits.

Three types of production order are being considered<sup>17</sup>:

- General production order
- Specific production order for traffic data
- Specific production order for CNA and LSPID data

---

<sup>15</sup> *Consultation Document* – Pg. 18.

<sup>16</sup> *Ibid.* – Pg. 10.

<sup>17</sup> *Ibid.* – Pg. 10.

### **General Production Orders**

PIAC does not support the creation of production orders in the absence of clear evidence showing how existing warrant powers (supplemented with assistance orders where necessary) are insufficient. Such evidence has yet to be provided.

The need for anticipatory orders, permitting law enforcement agencies to monitor transactions for a specified period of time, is also insufficiently documented. In any case, we cannot perceive a situation in which any such order would or should require a different standard than currently applies to search and seizure, or to interception of communications.

If general production orders are nevertheless created, they should be subject to the same procedural safeguards as currently apply to search warrants (or interception, where appropriate). To apply any lower standard would be to go beyond the objective of *maintaining* existing lawful access capabilities, in the new electronic environment.

### **Production Orders for "Traffic Data"**

It is suggested that issuance of specific production orders would be subject to a lower standard than that for issuance of general production orders. In particular, the Consultation paper suggests that "the standard for Internet traffic data should be more in line with that required for telephone records and dial number recorders in light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication".<sup>18</sup>

PIAC disagrees. First, it is not at all clear how "traffic data" in the Internet context could be stripped of content that is not available in the telephone context. Second, it is not clear that individuals have a low expectation of privacy in respect of their Internet address, at least once they know what other information about them could, or would necessarily, be transmitted along with Internet address information.

The Lawful Access Consultation document does not define traffic data. However, a definition is found in The Council of Europe Convention on Cyber-Crime. Under the Convention, traffic data is defined as, "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."<sup>19</sup>

It is notable that the explanatory memorandum to the Convention cautions against the simplistic notion that Internet "traffic data" can be easily separated from more substantive information in which a higher expectation of privacy exists:

---

<sup>18</sup> p.12.

<sup>19</sup> The Council of Europe Convention on Cyber-Crime, Article 1(d)

“... the privacy interest is generally considered to be less with respect to the collection of traffic data than interception of content data. Traffic data about time, duration and size of communication reveals little personal information about a person or his or her thoughts. However, a stronger privacy issue may exist in regard to data about the source or destination of a communication (e.g. the visited websites). The collection of this data may, in some situations, permit the compilation of a profile of a person's interests, associates and social context. Accordingly, Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures...”<sup>20</sup>

It has become apparent during the course of this consultation that it simply is not possible to clearly separate ‘traffic’ data from ‘content’ data (i.e., data that reveals much more about an individual) in the internet context. See A Pascual's “Access to traffic data: when reality is far more complicated than a legal definition.”<sup>21</sup> What looks like mere “traffic data” to a computer layperson, for example, could be a wealth of personal information in the hands of a computer expert.

Given that internet ‘traffic data’ can be so rich in information about an person's lifestyle, interests, views, etc., the standard for lawful access to such data should be at least as high as currently required for interception of communications or searching of records. Otherwise, the government will not be *maintaining* current standards of lawful access, but will in fact be *expanding* them.

As noted by the Privacy Commissioner of Canada, George Radwanski, “Agents of the state in Canada cannot order Canada Post to photocopy the address on every envelope we send, nor can they order bookstores to keep a record of every book we buy, let alone of every page of every magazine we leaf through. There is no reason why they should be able to exercise such powers with regard to every e-mail someone sends or every Web site he visits.”<sup>22</sup>

## Preservation Orders

Preservation orders do not currently exist in Canadian law. They are being proposed pursuant the Council of Europe *Convention*, so as to provide law enforcement with a further tool of access. A preservation order would require the service providers to store and save existing data specific to a transaction or client. The order would be temporary, remaining in effect only as long as it takes law enforcement agencies to obtain a judicial warrant to seize the data or a production order to deliver the data.<sup>23</sup>

<sup>20</sup> *Explanatory Memorandum to the Convention on Cyber-Crime*, para. 221.

<sup>21</sup> <http://www.it.kth.se/~aep/private/cnglobal2002-escuderoa.ppt>

<sup>22</sup> *Comments of the Privacy Commissioner of Canada on Lawful Access*, November 25<sup>th</sup>, 2002.

<sup>23</sup> *Consultation Document* – Pg. 14.

No data has been provided to justify the creation of this new order, which constitutes a limited form of data retention. Without clear justification, it should not be adopted.

While the proposed Preservation Order does not raise the same concerns as would routine, longer-term retention of data as proposed in other jurisdictions, it is a step in that direction and could become a "back door" method of obtaining judicial authorization for access, circumventing the higher thresholds that would apply for standard warrants.

We do not believe that a clear case has been made to support the introduction of data-preservation orders. No statistics have been introduced, no rationale has been offered beyond simple reference to the Council of Europe Convention on Cyber-Crime. In any case, the creation of this new type of order would clearly constitute an expansion, rather than a maintenance, of existing lawful access capabilities, and should be rejected on that basis alone.

## Virus Dissemination

The Council of Europe Convention on Cyber-Crime requires signatory states to criminalize the creation, sale and possession without right of devices (e.g., computer programs) that are designed or primarily adapted for the purpose of committing offences specified in the Convention, whether or not the virus has been deployed or has caused any form of mischief.

Further, in order to ratify the Convention, new offences in relation to illegal devices (such as viruses) would have to be added. These could include importation, procurement for use, and otherwise making available an illegal device as defined in the Convention.

We generally support the prohibition against viruses, as contemplated by the government. However, we have some concerns about the application of the proposal with respect to a virus that has not been deployed and has not caused any mischief. Some software or devices, due to programming errors (commonly referred to as 'bugs') or poor programming technique may fall within scope of this prohibition. Care should be taken to appropriately circumscribe the definition of virus and non-deployed or contingent virus.

In addition, care must be taken not to prohibit the legitimate activities of individuals and companies that possess these devices for analytical, research, design, educational, or anti-virus purposes. Nor should a person be guilty of an offence if they have an undetected virus or other device residing on their computer without their knowledge. Any provision outlawing possession of viruses should be carefully drafted so as to ensure that innocent individuals will not be caught.

## Extra-Territoriality

The consultation paper details that the Council of Europe Convention on Cyber-Crime calls for the criminalization of certain offences relating to computers, the adoption of procedural powers in order to investigate and prosecute cyber-crime, **and the promotion of international cooperation through mutual legal assistance and extradition in a criminal realm that knows no borders.**<sup>24</sup>

We have serious concerns regarding the risk of Canadians being subject to non-Canadian laws based upon a request from another jurisdiction. Canadian law enforcement officials should only enforce Canadian laws and not assist in the enforcement of foreign laws that are substantially different.

## Conclusion

The Canadian government, through the *Canadian Electronic Commerce Strategy* and the policy objectives of the *Telecommunications Act* has actively encouraged the adoption of new technologies within the Canadian marketplace. Indeed, we rank ahead of many other countries in terms of penetration and user acceptance and even cost in the internet and telecommunication sectors. These accomplishments have brought Canada well deserved praise as well as obvious economic benefit. It would seem that these same new technologies are now being used to justify a potentially invasive state surveillance regime under the guise of 'lawful access'.

We agree that new technologies necessitate updated legislation, so as to ensure that they are not inappropriately excluded from existing provisions. However, we do not see any reason why electronic mail should be subject to a lower standard of protection than telephone calls or regular mail. We do not see why Internet browsing should be subject to a lower standard of protection than book purchasing or researching in a library. We do not see why our movements should be subject to tracking merely because we choose to use a cellular phone or other wireless device.

Canadians should not be subject to greater monitoring or scrutiny just because they choose to avail themselves of new technologies and convenience. Criminal law principles, including standards for lawful access, should be technology-neutral.

Throughout this consultation process the government has not demonstrated why the proposed measures are necessary, how they are reasonable or that there are no less-intrusive alternatives. Such evidence is required in order to meet the test set out in the *Charter of Rights and Freedoms*, as well as to convince civil society of the appropriateness of the proposed measures. After a

---

<sup>24</sup> Consultation Document – Pg. 5.



**PIAC Lawful Access Consultation Submission**

review of the consultation paper and participation in the roundtable activities, we find ourselves left with more questions than answers. We cannot support the proposed new measures for lawful access in their current form given the lack of supporting data, the lack of adequate privacy safeguards inherent in them, and the significant expansion in lawful access that they would permit for one type of technology. We do not believe that the proposals, as currently constituted, meet the test set out by the Supreme Court of Canada for reasonable and demonstrably justified limits on the right to be free from state surveillance.

We therefore call upon the government to take the following steps, if it wishes to pursue this matter further:

- Publish all background materials relating to the Council of Europe Convention on Cyber-Crime, including documents detailing Canada's position, and explanatory memoranda relating to the Canadian implementation of the convention;
- Provide empirical evidence and full justification for all components of the lawful access proposals;
- Publish draft legislation and accompanying regulations for further consideration and feedback by stakeholders, so that we know what precisely is being proposed;
- Allow sufficient time for a full, thorough and informed public consultation.

All of which is respectfully submitted,

*original signed*



s.19(1)

Public Interest Advocacy Centre

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 17 12:18 PM  
To: la-al@justice.gc.ca  
Cc: [REDACTED]  
Subject: Comments re: Lawful Access

Our client, AXIA SuperNet Ltd. will be forwarding you comments in the next couple of days in response to the Lawful Access Consultation Paper. Could you please confirm via e-mail that you will consider these comments.

Thanks you.

[REDACTED]  
Davis & Company, Edmonton  
T 780 429-6805  
F 780 428-1066  
email: [REDACTED]

Please visit our website at: [www.davis.ca](http://www.davis.ca)

This e-mail is privileged and contains confidential information intended only for the person(s) named above. Any other distribution, copying or disclosure is strictly prohibited. If you have received this e-mail in error, please notify me immediately by telephone and delete the electronic and any hard copies.

Company  
No att.

**Pierlot, Paul**

---

**From:** [REDACTED]  
**Sent:** 2002 Dec 17 2:57 PM  
**To:** la-al@justice.gc.ca  
**Cc:** [REDACTED]  
**Subject:** Lawful Access Consultation

s.19(1)



Telesat Canada Lawful

Access C...

Attached please find the comments of Telesat Canada, submitted in response to the above referenced consultation document on Lawful Access.

The file is in PDF format (427KB).

Thank you.

[REDACTED] - Regulatory Affairs

(613) 748-8700 ([REDACTED])

<<Telesat Canada Lawful Access Comments Final .pdf>>



Telesat Canada  
1601 Telesat Court  
Gloucester, Ontario  
K1B 5P4

December 17, 2002

*Via e-mail: la-al@justice.gc.ca*

Lawful Access Consultation  
Criminal Law Policy Section  
5<sup>th</sup> Floor, 284 Wellington Street  
Ottawa, Ontario  
Canada, K1A 0H8

Dear Sir/Madam:

**Re: Lawful Access – Consultation Document**

Telesat Canada ("Telesat" or "the Company") is pleased to provide the following comments on the *Lawful Access – Consultation Document* ("the *Consultation Document*" or "the *Document*"), dated August 25, 2002, and released by the Department of Justice, Industry Canada, and Solicitor General Canada ("the Departments").

The lawful access issues addressed in the *Consultation Document* are of importance to all Canadians, and Telesat is firmly of the view that, to the extent that telecommunication service providers' network facilities may be directly involved in the carriage of information or communications of an illicit nature, it is incumbent on those service providers to provide all reasonable assistance to Canadian law enforcement agencies to gain access to this illicit information or communication, consistent with the *Canadian Charter of Rights and Freedoms* and other pertinent legislation.

By the same token, until there is a reasonable expectation that particular service providers' networks or services may be involved in the carriage or transmission of such traffic, or where there exist other more logical and cost-effective network points to provide the desired access capability, it would not be reasonable for that particular facility or service provider to spend money to develop any such technical access capability for these networks or services, assuming it was even technically feasible to do so. In these instances, no law enforcement or other public interest benefit would result from providing this capability; rather, the effect would simply be to drive up those service providers' costs, and ultimately the prices they must charge their customers.

As discussed in more detail below, Telesat believes that the majority of services provided by fixed satellite services ("FSS") facilities are unrelated or cannot be connected to the covert, illicit activities of concern in the *Consultation Document*. Moreover, for those few instances where FSS services could be involved in the carriage of such communications, it is generally in conjunction with terrestrial networks which provide the end user and switching portions of the service, and which would provide the more logical and cost-effective access points to these private communications. In this regard, it is Telesat's understanding that the specific information which U.S. legislation requires for surveillance is primarily obtained through carriers operating switching facilities, and not FSS facility providers.

As a preliminary matter, Telesat would also note that the *Document* is written from a high-level perspective. For all the issues of concern to be fully examined and understood, the Company believes that further public consultation by the Departments is required, once specific details on possible legislative proposals and regulations have been provided, before any formal legislation is actually introduced.

In what follows, Telesat will first provide general background information on the nature of its telecommunications network facilities and services, and then provide specific comment on certain issues raised in the *Consultation Document* of particular concern to the Company. Telesat will provide its comments from a satellite provider's perspective.

## **BACKGROUND**

Telesat was created in 1969 and is recognized as a world leader in satellite communications and system design. Over its more than 30 years of existence, Telesat has designed and operated six generations of FSS satellites, as well as a Direct Broadcast Satellite ("DBS"), bringing satellite communications services to all regions of Canada, including the far North. Telesat's current fleet of satellites consists of three FSS and one DBS satellite. A second Telesat DBS satellite will be launched later this month, and a second FSS satellite in the Anik F series is scheduled for launch in the third quarter of 2003. Telesat has spent well in excess of a billion dollars on the DBS and Anik F series of satellites over the past few years. The Company currently employs approximately 500 highly trained people across Canada, and its annual revenues are in excess of \$300 million.

Until March 1, 2000, Telesat had an exclusive mandate in the provision of domestic and Canada-U.S. cross-border FSS facilities. With the implementation of the 1997 World Trade Organization agreement on trade in basic telecommunications services, this mandate came to an end. Currently more than 50 foreign-owned and operated satellites have been placed on Industry Canada's approved FSS list to provide competitive satellite services anywhere in Canada. While meeting the competitive challenge in its home markets, Telesat has also expanded its area of operations to include all of North and South America.

Telesat provides satellite-based services through four strategic business units:

**Broadcast Services:** Telesat's broadcast services are comprised of point-to-point and point-to-multi-point satellite broadcast distribution of television programs, video signals, and other services including special events and live reports. Within Canada, more than 400 television and radio signals are distributed by Telesat satellites on a full-time basis. Almost all of the Canadian television broadcasts distributed to cable companies, Direct-to-Home ("DTH") and other end-users in Canada are at some point carried by Telesat.

**Business Networks Services:** Telesat provides satellite-based, private-line wireless data networks nation-wide and related ground segment and maintenance services to a broad range of financial, retail, industrial and commercial companies and government organizations which require voice, data and video applications. Business networks services applications include point-of-sale, electronic banking, airline and travel reservations, retail inventory management, video conferencing, distance education, LAN-to-LAN connectivity, Internet and intranet requirements and private voice networks.

**Carrier Services:** Telesat provides satellite voice and data transmission services which enable telephone companies (such as Bell Canada and Northwestel Inc.) to utilize satellite communications as part of their domestic telephone networks to provide telephone and data services to remote areas such as northern Canada. The Company also provides satellite capacity to foreign customers for linking high-speed Internet traffic between the United States and South America.

**International Consulting Programs:** With over 30 years of engineering and technical experience, Telesat is a leading consultant in the establishment, operation and upgrading of satellite systems world-wide, having provided consulting services to businesses and governments in more than 30 countries. Telesat has developed a wide range of specialized services designed to assist satellite operators, spacecraft manufacturers and companies involved in the field of satellite communications.

In terms of 2001 revenues, broadcast services accounted for approximately 54 percent of total Telesat revenues; business networks services accounted for 27 percent; carrier services accounted for nine percent; and international consulting programs accounted for 10 percent.

## SPECIFIC COMMENTS

As stated in the *Consultation Document*:

It is proposed that all service providers (wireless, wireline, and Internet) be required to ensure that their systems have the technical capability to provide lawful access to law enforcement and national security agencies....

The central tenet of the proposal is that service providers would be required to have the technical capability to provide access to the entirety of a specific telecommunication transmitted over their facilities, subject to lawful authority to intercept. This would include the content and the telecommunications-associated specific data associated with that telecommunication. [*Consultation Document* at page 7]

Based on this and other language in the *Document*, it is Telesat's understanding that the lawful access legislation and regulations would apply to all telecommunications service providers, including carriers, resellers, and Internet service providers, and that these service providers would generally be required to engineer their networks or facilities so as to allow law enforcement agencies to intercept specific telecommunications transmissions as well as to provide certain related telecommunications transmission data and customer information. It is also the Company's understanding that service providers may be required to retain certain transmission data and customer information pursuant to a preservation order of a limited time duration, but would not themselves be required to record the actual content of any transmission. The Company further understands that service providers would not be responsible for the costs of any change to their existing systems or networks necessary to allow the intercept or data collection capabilities, but may be responsible, on a going forward basis, for those costs for any significant upgrades to their facilities or for any new technologies and services introduced by the service provider.

### **FSS Services are Typically Delivered to Other Telecom Service Providers**

In attempting to satisfy the technical access requirements, it must be pointed out that satellite-based non-broadcasting services, and particularly the satellite services of the type provided by FSS facilities providers, typically differ and are based on different protocols from those used by other wireline and wireless service providers. Typically the satellite service being provided is a dedicated, 24-hour or "always-on" service over the life of the service contract, which in some situations may be for the life of the satellite (e.g., 12 to 15 years). Some services, notably those providing business services to end-users, utilize hubs on Company premises but Telesat does not today have access to the individual signals either because the compression/multiplexing/encryption protocols are

not available other than as a digital stream or because the hub does not process the signal itself but only provides switching capability between remote terminals.

In many instances the customer also owns and operates their own earth station facilities for both uplinking and downlinking the telecommunications signal, without any Company-provided hubs, meaning that the satellite provider has no terrestrial facility in place through which that customer's communications transmission would pass. That being the case, satellite operators typically would not have either the switching equipment nor the telecommunications associated data-recording or collection capabilities that other service providers typically rely on to deliver their services.

Telesat would also note that where FSS facility providers are now involved in the provision of telephony or Internet services, it is generally in the role of a carrier's carrier. In this role, the satellite operator typically provides a long-haul transmission service to remote regions located within a conventional telephone company's operating territory, but does not provide a service directly to the end user. Acting in this role as a wholesaler of bulk capacity, it would be impossible for the satellite operator to provide interception capabilities targeting a specific end user, or even to provide any telecommunications associated data on a specific end user in any meaningful manner. Rather, the only cost-efficient and effective way to intercept these communications would be through the networks of the service provider providing the switching capability or the facility to the end user. Therefore, in developing the legislation, the Government should provide sufficient flexibility to distinguish between a carrier providing an isolated component and the end-service provider (including, for example, an Internet service provider ("ISP")) where it may be more appropriate to intercept the communication.

Further to this point, and unique to satellite, even knowing the destination or termination of certain satellite-based services can be problematic. For example, because of the broadcast nature of satellite services, that service could be received by an earth station, or any number of earth stations, located anywhere within the coverage footprint of the satellite. In the case of Telesat's satellites that could be anywhere in Canada. Indeed, some of the Company's satellites have footprints that cover all of North and South America.

It is noteworthy that theoretically it may be possible to receive any signal within a satellite footprint through the use of a satellite dish within that footprint, including a dish specifically deployed for law enforcement purposes. However, the security provided individual signals comes from the protocols used to compress, multiplex and encrypt those signals. In cases of private communications where the satellite operator does not control those protocols, the operator will be not be able to provide the access required for law enforcement agencies to intercept those communications, other than to indicate that some form of signal was being transmitted.

In sum, there are definite limits as to what the FSS operator can do in these situations to provide technical access capabilities. In particular, satellite operators generally cannot decrypt, decipher or demodulate the signals being carried over their networks where the



operator does not control the protocols. Surveillance is therefore only possible if it is carried out at control points outside of satellite operators' networks.

### **Cost Implications would be Significant**

Given the high level discussion in the *Document*, Telesat cannot make financial estimates as to the precise costs that would have to be incurred to provide these technical access capabilities, either for existing satellite networks or services or for upgraded or new services or systems. However, given that little work or study has been conducted in these areas and that solutions designed for terrestrial networks and services may be of limited use or value in a satellite environment, it is reasonable to expect that it would be necessary to develop satellite-specific capabilities, and thus it would be costly to ensure that law enforcement agencies could gain the required access to all satellite networks and services.

In this regard, Telesat would further note that the Canadian satellite market is a relatively small market, and that, to the extent equipment manufacturers are willing to design and incorporate access capabilities into their products, they will be largely driven or motivated to do so by developments and mandated requirements in the larger non-Canadian markets. If compliance costs are to be minimized in Canada, it is therefore important that the requirements ultimately adopted in Canada take into account what is being required in, and being built for, these other satellite jurisdictions.

Moreover, requiring Canadian FSS operators to incur any significant costs to provide lawful access capabilities would place them at a competitive disadvantage vis-à-vis their foreign competitors unless the same requirements were imposed on all satellites operating in Canada. As noted above, there are currently more than 50 foreign-owned and operated FSS satellites on Industry Canada's approved satellite list to provide service in Canada. Few, if any, of these foreign satellite operators have any network infrastructure on the ground in Canada, making it difficult for Canadian law enforcement agencies to gain access to any Canadian information and communications of concern which might be carried by those facility providers.

Even if the lawful access requirements were implemented so as to apply only to new services or a significantly upgraded service as suggested would be the minimum requirement at page 8 of the *Document*, their application only to Canadian satellite operators and not to the foreign satellite operators who also have coverage of Canada, would have similar adverse consequences for the Canadian operators, either by increasing the cost of their new or upgraded services or by reducing or removing the incentive for these operators to introduce or consider innovative new or upgraded services.

Telesat notes that the need for equitable treatment of Canadian industry players is expressly recognized in *Consultation Document*:

The public policy objectives of this process are to maintain lawful access capabilities for law enforcement agencies and national security agencies in the face of new technologies and to preserve and protect the privacy and other rights and freedoms of all people in Canada. In striving to attain these goals, *it is essential that no competitive disadvantages are placed on Canadian industry and that the solutions adopted do not place an unreasonable burden on the Canadian public.* [Consultation Document at page 6, emphasis added]

In the context of Canadian satellite markets, to ensure that no competitive disadvantages are placed on Canadian market participants, it is imperative that the same technical access requirements are imposed on all foreign satellite operators who wish to operate within Canada. Indeed, if the same requirements do not apply to these operators, not only will Canadian satellite operators be placed at a severe competitive disadvantage, but the Canadian legislation will be rendered ineffectual in its application to satellite facilities, as criminal or other groups posing public safety risks in Canada could simply use these foreign satellites for their illicit activities – i.e., “intercept safe-havens” for this possible illicit activity will have been created.

In this regard, Telesat would further note that, while FSS facility providers operating in the United States are subject to that country's *Communications Assistance for Law Enforcement Act* (“CALEA”), the practical application of that legislation drives law enforcement agencies to conduct surveillance through common-carrier switching facilities, and not the FSS operator. Accordingly, no attempt has been made to force these carriers to unnecessarily re-engineer their networks to provide technical access capabilities. Indeed, *CALEA* is very specific as to the information to be captured in order to be compliant with these requirements, and generally none of this pertains to FSS services.

Telesat appreciates the opportunity to provide these comments, but would urge the Departments to hold another round of public consultations before any formal legislation is introduced, once all the comments received in this stage of the review have been considered and more specific details on possible legislative proposals and regulations have been provided. Telesat would be pleased to participate in that further proceeding and is available to discuss any of these matters further.

Yours truly,



s.19(1)

– Regulatory & Government Initiatives

**Pierlot, Paul**

---

**From:** [REDACTED] s.19(1)  
**Sent:** 2002 Dec 17 7:27 PM  
**To:** la-al@justice.gc.ca  
**Subject:** PovNet's submission to the Lawful Access Consultation



doj submission.doc

Please find attached PovNet's submission to the Lawful Access Consultation process. We apologize that we missed the deadline; could you send us an acknowledgement that you have received our submission.

Thank you.

--  
[REDACTED]  
PovNet  
604-876-8638  
<http://www.povnet.org>



Suite 800, 1281 W. Georgia Street  
Vancouver, B.C. V6E 3J7  
(604) 876-8638 (ph); (604) 685-7611 (fax)  
povnet@povnet.org  
<http://www.povnet.org>

December 16, 2002

Lawful Access Consultation,  
Criminal Law Policy Section  
5th Floor, 284 Wellington St.,  
Ottawa, Ontario, Canada, K1A 0H8.

To whom it may concern:

*Regarding: The Proposed Lawful Access Legislation*

PovNet is an online resource for anti-poverty advocates. We host a public web site and a series of confidential email lists that enable lawyers and community advocates to consult with each other about difficult cases, law reform issues, and other sensitive matters. Our lists and web site are hosted by the Vancouver Community Network (VCN). We are particularly concerned about this proposed legislation as it affects interception of confidential communications from third parties.

Like s. 488.1 of the Criminal Code, which was struck down by the Supreme Court of Canada as a violation of s. 8 of the Charter because of its impact on solicitor client privilege, the lawful access proposal would violate the privacy of advocates and others who use the internet.

Moreover, because of the nature of email and email lists, the violation could not be limited to just the individual who is the subject of an investigation. If such a person were a member of a confidential list, every message posted to the list would be sent to the person's inbox and thereby be included in the records to be accessed. The vast majority of these messages would have nothing whatever to do with the target, but all of them would end up in the hands of the authorities under the proposed measures. No technological measure would be possible to prevent this, or to allow the third parties to protest the disclosure. The interception of telephone conversations poses no similar danger. This suggests that legal protections for email interceptions must be at equal to those for telephone wiretaps, if not greater.

---

Steering Committee: BC Coalition of People with Disabilities, BC Library Association, BC Public Interest Advocacy Centre, Community Legal Assistance Society, End Legislated Poverty, federated anti-poverty groups of bc, Inland Refugee Society, Legal Services Society, MOSAIC, Social Planning and Research Council of BC, Tenants Rights Action Coalition

FUNDED BY LAW FOUNDATION; VANCOUVER FOUNDATION; LEGAL SERVICES SOCIETY; LIBRARY SERVICES BRANCH, COMMUNITIES CONNECT PROGRAM; AND OFFICE OF LEARNING TECHNOLOGIES, COMMUNITY LEARNING NETWORKS INITIATIVE

Advocates rely on PovNet to be a confidential resource for them; we are extremely concerned that the legislation that you are proposing would violate this confidentiality.

Yours sincerely,

s.19(1)

PovNet

Pierlot, Paul

s.19(1)

From: [REDACTED]  
Sent: 2002 Dec 18 2:11 PM.  
To: 'la-al@justice.gc.ca'  
Subject: RE: Lawful Access - Consultation Document - RWI Comments

Could you please let me know when and where I would find the Comments of other parties with regard to this Consultation.

Thank You

[REDACTED]  
Executive Assistant  
Government & Intercarrier Relations  
Rogers Wireless Inc.  
Phone: 416-935-7212  
BlackBerry: [REDACTED]

> -----Original Message-----

> From: [REDACTED]  
> Sent: Monday, December 16, 2002 4:20 PM  
> To: 'la-al@justice.gc.ca'  
> Cc: [REDACTED]  
> Subject: Lawful Access - Consultation Document - RWI Comments

> ELECTRONIC FILING SUMMARY:

> 2002/12/16 - Rogers Wireless Inc.  
> Lawful Access - Consultation Document  
> DESCRIPTION: Letter to Industry Canada

> FILE NAMES:

> Lawful Access Dec 16 Letter.pdf - 30 KB (Adobe Document)  
> Lawful Access Dec 16 Comments.pdf - 158 KB (Adobe Document)

> << File: Lawful Access Dec 16 Letter.pdf >> << File: Lawful Access Dec  
> 16 Comments.pdf >>

> If you have any problems accessing the attached, please call Cindy Hicks  
> at 416-935-7212.

> \*\*\*\*\*  
> \*\*\*\*\*  
> This email may contain privileged, confidential or undisclosed  
> information. If the reader of this email is not the intended recipient or  
> an agent responsible for delivering it to the intended recipient, you are  
> hereby notified that you have received this email in error, and that any  
> review, dissemination, distribution or copying of it is strictly  
> prohibited. If you have received this in error, please notify us  
> immediately via return email. Thank  
> you.\*\*\*\*\*  
> \*\*\*\*\*